PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

PROTECTING MOBILE PRIVACY: YOUR SMARTPHONES, TABLETS, CELL PHONES AND YOUR PRIVACY

Before the

UNITED STATES SENATE

COMMITTEE ON THE JUDICIARY

SUBCOMMITTEE FOR PRIVACY, TECHNOLOGY AND THE LAW

Washington, D.C.

May 10, 2011

Chairman Franken, Ranking Member Coburn, and members of the Subcommittee, my name is Jessica Rich and I am the Deputy Director of the Bureau of Consumer Protection at the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate this opportunity to appear before you today to discuss the Commission's efforts to protect consumers' privacy in the mobile arena.

This testimony first broadly surveys the growth of the mobile marketplace and the Commission's response to this developing industry. Second, it highlights four of the Commission's recent law enforcement actions in the mobile arena, one involving statements that a public relations agency made in the iTunes mobile application store, another involving unsolicited commercial texts, and two recent privacy enforcement actions involving Google and Twitter, major companies in the mobile arena. Finally, it describes the Commission's efforts to address the privacy challenges of these new, and often very personal technologies, including a discussion of how mobile technology is addressed in the privacy framework recently proposed by FTC staff.

I. The Mobile Marketplace

Mobile technology is exploding with a range of new products and services for consumers. 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.[2] Also by that

[1] While the views expressed in this statement represent the views of the Commission, my oral presentation and responses to questions are my own and do not necessarily reflect the views of the Commission or any individual Commissioner.

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

same time, 27 percent of U.S. mobile subscribers owned a smartphone,[3] 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 can not only make telephone calls, but also offer web browsing, e-mail, and a broad range of data services. These new popular mobile devices allow consumers to handle a multitude of tasks in the palm 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.[4] Consumers can search mobile 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. Consumers can join texting programs that provide instantaneous product information and mobile coupons at the point of purchase. Consumers can download mobile software applications ("apps") that can perform a range of consumer services such as locating the nearest retail stores, managing shopping lists, tracking family budgets, or calculating tips or debts. Apps also allow consumers to read news articles, play interactive games and connect with family and friends via

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

[4] 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 Vast Majority of Marketers Will Utilize Mobile Marketing and Increase Spending on Mobile Platforms in 2011,* ANA Press Release describing the results of a survey conducted by the Association of National Advertisers in partnership with the Mobile Marketing Association, dated January 31, 2011, *available at* www.ana.net/content/show/id/20953.

social media applications. 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. Although there are no special laws applicable to mobile marketing that the FTC enforces, the FTCs core consumer protection law – Section 5 of the FTC Act – prohibits unfair or deceptive practices in the mobile arena.[5] This law applies to marketing in all media, whether traditional print, telephone, television, desktop computer, or mobile device.

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.[6] In addition, in November 2006, the Commission held a three-day technology forum that prominently featured mobile issues.[7] 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.[8] And in 2008, the Commission

---

[5] 15 U.S.C. § 45(a).

[6] 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.

[7] 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.

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

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.[9]

More recently, the agency has invested in new technologies to provide its investigators and attorneys with the necessary tools to monitor and respond to the growth of the mobile marketplace. For example, the Commission has established a mobile technology laboratory, akin to the Commission's longstanding Internet investigative laboratory, containing a variety of smartphones utilizing different platforms and carriers, as well as software and equipment that permit FTC investigators to collect and preserve evidence and conduct research into a wide range of mobile issues, including those related to consumer privacy.

III. Applying the FTC Act to the Mobile Arena

Law enforcement is the Commission's most visible and effective tool for fighting online threats, including those in the mobile marketplace. As described below, the FTC has brought four recent cases that illustrate how Section 5 applies to the mobile arena, including unsolicited text messages and the privacy and security of data collected on mobile devices.

In August 2010, 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.[10] The company allegedly posted positive reviews of gaming apps using account names that gave the impression the reviews had been submitted by

---

Workshop on Consumer Privacy and Data Security, available at www.ftc.gov/bcp/workshops/transatlantic/index.shtml.

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

[10] *Reverb Commc'ns, Inc.*, FTC Docket No. C-4310 (Nov. 22, 2010) (consent order).

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 connection 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.

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 used 32 pre-paid cell phones to send over 5 million unsolicited text messages – almost a million a week – to the mobile phones of U.S. consumers.[11] Many consumers who received Flora's text messages – which typically advertised questionable mortgage loan modification or debt relief services – had to pay a per-message 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.[12] The Commission

---

[11] *FTC v. Flora*, CV11-00299 (C.D. Cal.) (Compl, filed Feb. 22, 2011).

[12] 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.

charged Flora with the unfair practice of sending unsolicited text messages and with deceptively claiming an affiliation with the federal government in connection with the loan modification service advertised in the text messages.[13]

The FTC has also taken action against companies that fail to protect the privacy and security of consumer information. Two recent cases highlight the FTC's efforts to challenge deceptive claims that undermine consumers' privacy choices in 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.[14] 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, if Google changes a product or service in a way that makes consumer information more widely available, it must seek affirmative express consent to such a change. This provision applies to *any* data collected from or about consumers, including mobile data. In addition, the order requires Google to implement a comprehensive privacy program and conduct independent audits every other year for the next 20 years.

---

[13] The complaint against Flora also alleges violations of the CAN-SPAM Act for sending unsolicited commercial email messages advertising his texting services that did not include a valid opt-out mechanism and failed to include a physical postal address. In these emails, Flora offered to send 100,000 text messages for only $300. *See* FTC Press Release, *FTC Asks Court to Shut Down Text Messaging Spammer* (Feb. 23, 2011), *available at* www.ftc.gov/opa/2011/02/loan.shtm.

[14] *Google, Inc.*, FTC File No. 102 3136 (Mar. 30, 2011) (consent order accepted for public comment).

Second, in the Commission's case against social networking service Twitter, the FTC charged that serious lapses in the company's data security allowed hackers to obtain unauthorized administrative control of Twitter.[15] 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 applications, prohibits misrepresentations about the extent to which Twitter protects the privacy of communications, requires Twitter to maintain reasonable security, and mandates independent, comprehensive audits of Twitter's security practices.

These are just two recent examples of cases involving mobile privacy issues, but the Commission's enforcement efforts are ongoing.[16] Staff has a number of active investigations into privacy issues associated with mobile devices, including children's privacy.

IV. Mobile Privacy Policy Initiatives

As noted, the rapid growth of mobile technologies has led to the development of many new business models involving mobile services. On the one hand, these innovations provide valuable benefits to both businesses and consumers. On the other hand, they facilitate 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

---

[15] *Twitter, Inc.*, FTC Docket No. C-4316 (Mar. 2, 2011) (consent order).

[16] *See also FTC v. Accusearch, Inc.,* 2007 WL 4356786 (D. Wyo. Sept. 28, 2007) (operation of a website that illegally obtained telephone records, including cell phone records, through pretexting was an unfair act) *,aff'd,* 570 F.3d 1187 (10th Cir. 2009).

facilitate data collection and sharing among many entities, including wireless providers, mobile operating system providers, handset manufacturers, application 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.[17] 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."[18] Further, the rush of on-the-go use, coupled with the small screens of most mobile devices, makes it even more unlikely that consumers will read detailed privacy disclosures.

In recent months, news reports have highlighted the virtually ubiquitous data collection by smartphones and their apps. Researchers announced that Apple has been collecting geolocation data through its mobile devices over time, and storing unencrypted data files containing this information on consumers' computers and mobile devices.[19] 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

---

[17] *See, e.g.*, Pew Internet & American Life Project, *Adults, Cell Phones and Texting* at 10 (Sept. 2, 2010), *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"); *Teens and Mobile Phones* at 73 (Apr. 20, 2010), *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).

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

[19] *See* Jennifer Valentino-Devries, *Study: iPhone Keeps Tracking Data*, WALL ST. J. (Apr. 21, 2011), *available at* http://online.wsj.com/article/SB10001424052748704570404576275323811369758.html.

device – that can then be used to track and predict consumers' every move.[20] Not surprisingly, 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.[21]

A. Privacy Roundtables

The Commission has been considering these and related issues in connection with its "Exploring Privacy" Roundtable series. 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.[22] During the second roundtable, one panel in particular focused on the privacy implications of mobile technology, addressing the complexity of data collection through mobile devices; the extent and

---

[20] *See, e.g.*, Robert Lee Hotz, *The Really Smart Phone*, WALL ST. J. (Apr. 23, 2011), *available at* http://online.wsj.com/article/SB10001424052748704547604576263261679848814.html?mod= (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* http://online.wsj.com/article/SB10001424052748704368004576027751867039730.html?mod= (documenting the data collection that occurs through many popular smartphone apps).

[21] NielsenWire, *Privacy Please! U.S. Smartphone App Users Concerned with Privacy When It Comes to Location* (Apr. 21, 2011), *available at* http://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* at 7 (Mar. 2011), *available at* http://aa-download.avg.com/filedir/other/Smartphone.pdf (64% of consumers worry about being tracked when using their smartphones).

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

nature of the data collection, particularly with respect to geolocation data; and the adequacy of privacy disclosures on mobile devices.[23]

B. Preliminary Staff Privacy Report

Based on the information received through the roundtable process, staff drafted a preliminary report ("Staff Report") proposing a new privacy framework consisting of three main recommendations, each of which is applicable to mobile technology.[24] First, staff recommends that companies should 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 is providing traffic and weather information to a consumer, it does not need to collect call logs or contact lists from the consumer's device. Further, although the app may need location information, the app developer should carefully consider how long the location information should be retained to provide the requested service.

Second, staff recommends that companies should 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 these choices and to ensure

---

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

[24] *See* FTC 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 Kovacic and Rosch issued concurring statements available at http://ftc.gov/os/2010/12/101201 privacyreport.pdf at Appendix D and Appendix E, respectively.

that they are understandable and accessible on the small screen. As stated in the Staff Report, companies should also obtain affirmative express consent before collecting or sharing sensitive information such as precise geolocation data.

Third, the Staff Report proposed a number of measures that companies should take to make their data practices more transparent to consumers, including improving disclosures to consumers about information practices. Again, because of the small size of the device, a key question staff posed in the report is how companies can create effective notices and present them on mobile devices.

After releasing the Staff Report, staff received 452 public comments on its proposed framework, a number of which implicate mobile privacy issues specifically.[25] FTC staff is

[25] *See* Comment of CTIA (Feb. 18, 2011), *available at* http://www.ftc.gov/os/comments/privacyreportframework/00375-58002.pdf; Comment of Verizon and Verizon Wireless (Feb. 18, 2011), *available at* http://www.ftc.gov/os/comments/privacyreportframework/00428-58044.pdf; *see also, e.g.*, Comment of Center for Digital Democracy and U.S. PIRG at 10-11, 20-21, 33 (Feb. 18, 2011), *available at* http://www.ftc.gov/os/comments/privacyreportframework/00338-57839.pdf; Comment of Stanford Security Laboratory at 11-12 (Feb. 18, 2011), *available at* http://www.ftc.gov/os/comments/privacyreportframework/00467-57980.pdf.

analyzing the comments and will take them in consideration in preparing a final report for release later this year.[26]

V. CONCLUSION

The Commission is committed to protecting consumers' privacy in the mobile sphere by bringing enforcement where appropriate and by working with industry and consumer groups to develop workable solutions that protect consumers while allowing innovation in this growing marketplace.

[26] Another major initiative addressing the mobile marketplace is the Commission's review of the Children's Online Privacy Protection Rule, issued pursuant to the Children's Online Privacy Protection Act ("COPPA"). Initiated in April 2010, this review sought public comment on whether technological changes to the online environment warrant any changes to the Rule or to the statute. 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. The Rule review is ongoing.