PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

THE NEED FOR PRIVACY PROTECTIONS:

PERSPECTIVES FROM THE ADMINISTRATION

AND THE FEDERAL TRADE COMMISSION

Before the

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

UNITED STATES SENATE

Washington, D.C.

May 9, 2012

I. Introduction

Chairman Rockefeller, Ranking Member Hutchison, and members of the Committee, I am Jon Leibowitz, Chairman of the Federal Trade Commission ("FTC" or "Commission").[1]

We are pleased to be testifying today alongside General Counsel Cameron Kerry of the Department of Commerce and the newest member of the FTC, Commissioner Maureen Ohlhausen. The Commission supports the privacy efforts and approach developed by the Department of Commerce, and we look forward to working with the Department of Commerce, the Administration, and Congress as they move forward in their efforts in this arena. Members of this Committee in particular have demonstrated that they understand how important it is that consumers' – and especially children and teens' – personal data be treated with care and respect.

This is a critical juncture for consumer privacy, as the marketplace continues to rapidly evolve and new approaches to privacy protection are emerging in the United States and around the world. After careful consideration, the Commission recently released the final privacy report ("Final Report"). The Final Report sets forth best practices for businesses to guide current efforts to protect consumer privacy while ensuring that companies can continue to innovate. The Commission urges industry to use this guidance to improve privacy practices and accelerate the pace of self-regulation. Importantly, we have seen promising developments by industry toward a Do Not Track mechanism and we ask the Committee to continue to encourage industry to move towards full implementation. The Report also calls on Congress to consider enacting general privacy legislation. We reiterate today our call to Congress to enact legislation requiring

[1] The views expressed in this statement represent the views of the Commission, with Commissioner J. Thomas Rosch dissenting and Commissioner Maureen K. Ohlhausen not participating. My oral presentation and responses to questions are my own and do not necessarily represent the views of the Commission or any other Commissioner.

companies to implement reasonable security measures and notify consumers in the event of certain security breaches, as well as targeted legislation that would provide consumers with access to information about them held by data brokers.

Privacy has been a key part of the Commission's consumer protection mission for more than 40 years. Throughout, the Commission's goal has remained constant: to protect consumers' personal information and ensure that they have the confidence to take advantage of the many benefits offered by the dynamic and ever-changing marketplace. To meet this objective, the Commission has undertaken substantial efforts to promote privacy in the private sector through law enforcement, education, and policy initiatives. For example, since 2001, the Commission has brought 36 data security cases; more than 100 spam and spyware cases; and 18 cases for violation of the Children's Online Privacy Protection Act ("COPPA"). The Commission has also brought highly publicized privacy cases against companies such as Google and Facebook and, most recently, Myspace. The Commission has distributed millions of copies of educational materials for consumers and businesses to address ongoing threats to security and privacy. And the FTC continues to examine the implications of new technologies and business practices on consumer privacy through ongoing policy initiatives, such as the Commission's Final Report.

This testimony begins by describing the Commission's Final Report. It then offers an overview of other recent policy efforts in the areas of privacy and data security and concludes by discussing the Commission's recent enforcement and education efforts.

II. Final Privacy Report

The FTC recently released its Final Report, setting forth best practices for companies that collect and use consumer data.[2] These best practices can assist companies as they develop and maintain processes and systems to operationalize privacy and data security practices within their businesses. To the extent these best practices exceed existing legal requirements, they are not intended to serve as a template for law enforcement or regulations under laws currently enforced by the FTC.[3]

The Final Report supports the three key principles laid out in the preliminary staff report.[4] Companies should adopt a "privacy by design" approach by building privacy protections into their everyday business practices. Such protections include providing reasonable security for consumer data, collecting only the data needed for a specific business

---

[2] FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf. Commissioner Rosch dissented from the issuance of the Final Privacy Report. He agrees that consumers ought to be given a broader range of choices and applauded the Report's call for targeted legislation regarding data brokers and data security. However, Commissioner Rosch has four major concerns about the privacy framework because he believes that: 1) in contravention of our promises to Congress, it is based on an improper reading of our consumer protection "unfairness" doctrine; 2) the current state of "Do Not Track" still leaves unanswered many important questions; 3) "opt-in" will necessarily be selected as the de facto method of consumer choice for a wide swath of entities; and 4) although characterized as only "best practices," the Report's recommendations may be construed as federal requirements. *See* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf at Appendix C.

[3] Information on the FTC's privacy initiatives generally may be found at business.ftc.gov/privacy-and-security.

[4] The Commission received over 450 public comments from various stakeholders in response to the preliminary report, which were highly informative to the Commission as it refined the final framework.

purpose, retaining data only as long as necessary to fulfill that purpose, safely disposing of data no longer in use, and implementing reasonable procedures to promote data accuracy.

Companies also should provide simpler and more streamlined choices to consumers about their data practices. Companies do not need to provide choice before collecting and using consumers' data for practices that are consistent with the context of the transaction, the company's relationship with the consumer, or as required or specifically authorized by law. For all other data practices, consumers should have the ability to make informed and meaningful choices at a relevant time and context and in a uniform and comprehensive way. The Commission advocated such an approach for online behavioral tracking – often referred to as "Do Not Track" – that is discussed in more detail below.

Finally, companies should take steps to make their data practices more transparent to consumers. For instance, companies should improve their privacy disclosures and work toward standardizing them so that consumers, advocacy groups, regulators, and others can compare data practices and choices across companies, thus promoting competition among companies. Consumers should also have reasonable access to the data that companies maintain about them, particularly for non-consumer-facing entities such as data brokers, as discussed in more detail below. The extent of access should be proportional to the volume and sensitivity of the data and to its intended use.

In addition, the Final Report makes general and specific legislative recommendations. The Report supports the development of general privacy legislation to ensure basic privacy protections across all industry sectors, and can inform Congress, should it consider such privacy

legislation.[5] The Commission recommends that any such legislation be technologically neutral and sufficiently flexible to allow companies to continue to innovate. In addition, the Commission believes that any legislation should allow the Commission to seek civil penalties to deter statutory violations. Such legislation would provide businesses with the certainty they need to understand their obligations as well as the incentive to meet those obligations, while also assuring consumers that companies will respect their privacy. We believe this approach would foster an environment that allows businesses to innovate and consumers to embrace those innovations without risking their privacy. The Final Report also calls on Congress to enact legislation requiring companies to implement reasonable security measures and notify consumers in the event of certain security breaches,[6] as well as targeted legislation for data brokers, discussed below. We look forward to working with Congress and other stakeholders to craft this legislation.

---

[5] Earlier this year, the Administration released its final "White Paper" on consumer privacy, recommending that Congress enact legislation to implement a Consumer Privacy Bill of Rights. *See Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[6] The Commission has long supported such federal data security and breach notice laws. *See, e.g.*, Prepared Statement of the FTC, *Data Security: Hearing Before the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Manufacturing, and Trade*, 112th Cong. (June 15, 2011), *available at* http://www.ftc.gov/os/testimony/110615datasecurityhouse.pdf; Prepared Statement of the FTC, *Protecting Social Security Numbers From Identity Theft*: *Hearing Before the Before the H. Comm. on Ways and Means, Subcomm. on Social Security*, 112th Cong. (Apr. 13, 2011), *available at* http://ftc.gov/os/testimony/110411ssn-idtheft.pdf; FTC, *Security in Numbers, SSNs and ID Theft* (Dec. 2008), *available at* http://www.ftc.gov/os/2008/12/P075414ssnreport.pdf; and President's Identity Theft Task Force, *Identity Theft Task Force Report* (Sept. 2008), *available at* http://www.idtheft.gov/reports/IDTReport2008.pdf.

The Report's recommendations broadly address the commercial use of consumer information, both online and offline, by businesses. Below, we highlight two specific issues addressed in the Report – Do Not Track and data brokers.

A. Do Not Track

The Final Report advocates the continued implementation of a universal, one-stop mechanism to enable consumers to control the tracking of their online activities across websites, often referred to as "Do Not Track," which the Commission first called for in December 2010 and Chairman Rockefeller has sought through his legislative proposal.[7] We recognize the benefits to such online data collection, including more relevant advertising and free online content that consumers have come to expect and enjoy. However, we have concerns that too many consumers either do not understand they are trading their privacy for free online content or have not made an informed choice to do so.

The Commission commends industry efforts to improve consumer control over behavioral tracking in response to our calls. As industry explores technical options and implements self-regulatory programs, and as Congress examines Do Not Track, the Commission continues to believe that an effective Do Not Track system should include five key principles. *First*, a Do Not Track system should be implemented universally to cover all parties that would track consumers. *Second*, the choice mechanism should be easy to find, easy to understand, and easy to use. *Third*, any choices offered should be persistent and should not be overridden if, for example, consumers clear their cookies or update their browsers. *Fourth*, a Do Not Track

[7] Do Not Track is intended to apply to third-party tracking of consumers because third-party tracking is inconsistent with the context of a consumer's interaction with a website; by contrast, most first-party marketing practices are consistent with the consumer's relationship with the business and thus do not necessitate consumer choice.

system should be comprehensive, effective, and enforceable. It should opt consumers out of behavioral tracking through any means and not permit technical loopholes.[8] *Fifth*, an effective Do Not Track system should go beyond simply opting consumers out of receiving targeted advertisements; it should opt them out of collection of behavioral data for all purposes other than those that would be consistent with the context of the interaction (*e.g.*, preventing click-fraud or frequency capping for ads). Such a mechanism should be different from the Do Not Call program in that it should not require the creation of a "Registry" of unique identifiers, which could itself cause privacy concerns. And unlike the Do Not Call Registry, a Do Not Track mechanism should be implemented by the private sector.

Early on, the companies that develop web browsers stepped up to the challenge to give consumers choices about how they are tracked online, sometimes known as the "browser header" approach. When consumers enable Do Not Track, the browser transmits the header to all types of entities, including advertisers, analytics companies, and researchers, that track consumers online. Just after the FTC's call for Do Not Track, Microsoft developed a system to let users of Internet Explorer prevent tracking by different companies and sites.[9] Mozilla introduced a Do

---

[8] For example, the FTC brought an action against a company that told consumers they could opt out of tracking by exercising choices through their browsers; however, the company used Flash cookies for such tracking, which consumers could not opt out of through their browsers. *In the Matter of ScanScout, Inc.*, FTC Docket No. C-4344 (Dec. 21, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023185/111221scanscoutdo.pdf.

[9] 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.

Not Track privacy control for its Firefox browser that an impressive number of consumers have adopted.[10] Apple subsequently included a similar Do Not Track control in Safari.[11]

The online advertising industry, led by the Digital Advertising Alliance ("DAA"), has also led efforts by implementing a behavioral advertising opt-out program. The DAA's accomplishments are notable: it has developed a notice and choice mechanism through a standard icon in ads and on publisher sites; deployed the icon broadly, with reportedly over 900 billion impressions served each month; obtained commitments to follow the self-regulatory principles from advertisers, ad networks, and publishers that represent close to 90 percent of the online behavioral advertising market; and established an enforcement mechanism designed to ensure compliance with the principles.[12] The DAA is also working to address one of the long-standing criticisms of its approach – how to limit secondary use of collected data so that the

---

[10] The Mozilla Blog, *Mozilla Firefox 4 Beta, Now Including "Do Not Track" Capabilities* (Feb. 8, 2011), blog.mozilla.com/blog/2011/02/08/mozilla-firefox-4-beta-now-including-do-not-track-capabilities/; Alex Fowler, *Do Not Track Adoption in Firefox Mobile is 3x Higher than Desktop*, MOZILLA PRIVACY BLOG (Nov. 2, 2011), http://blog.mozilla.com/privacy/2011/11/02/do-not-track-adoption-in-firefox-mobile-is-3x-higher-than-desktop/.

[11] Nick Wingfield, *Apple Adds Do-Not-Track Tool to New Browser*, WALL ST. J., Apr. 13, 2011, *available at* http://online.wsj.com/article/SB10001424052748703551304576261272308358858.html. Google has taken a slightly different approach – providing consumers with a browser extension that opts them out of most behavioral advertising on a persistent basis. Sean Harvey & Rajas Moonka, *Keep Your Opt Outs*, GOOGLE PUBLIC POLICY BLOG (Jan. 24, 2011), http://googlepublicpolicy.blogspot.com/2011/01/keep-your-opt-outs.html.

[12] Peter Kosmala, *Yes, Johnny Can Benefit From Transparency & Control*, SELF-REGULATORY PROGRAM FOR ONLINE BEHAVIORAL ADVERTISING, http://www.aboutads.info/blog/yes-johnny-can-benefit-transparency-and-control (Nov. 3, 2011); *see also* Press Release, Digital Advertising Alliance, *White House, DOC and FTC Commend DAA's Self-Regulatory Program to Protect Consumers Online Privacy* (Feb. 23, 2012), *available at* http://www.aboutads.info/resource/download/DAA%20White%20House%20Event.pdf.

consumer opt-out extends beyond simply blocking targeted ads and to the collection of information for other purposes. The DAA has released principles that include limitations on the collection of tracking data and prohibitions on the use or transfer of the data for employment, credit, insurance, or health care eligibility purposes.[13] The DAA is now working to fully implement these principles. Just as important, the DAA recently moved to address some persistence and usability criticisms of its icon-based opt out by committing to honor the tracking choices consumers make through their browser settings.[14]

At the same time, the World Wide Web Consortium ("W3C"), an Internet standards-setting body, has convened a broad range of stakeholders to create an international, industry-wide standard for Do Not Track, including DAA member companies; other U.S. and international companies; industry groups; and public interest organizations. The W3C group has done admirable work to flesh out how to make a Do Not Track system practical in both desktop and mobile settings as reflected in two public working drafts of its standards.[15] Some important issues remain, and the Commission encourages all of the stakeholders to work within the W3C group to resolve these issues.

---

[13] Digital Advertising Alliance, *About Self-Regulatory Principles for Multi-Site Data* (Nov. 2011), *available at* http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf.

[14] Press Release, Digital Advertising Alliance, *DAA Position on Browser Based Choice Mechanism* (Feb. 22, 2012), *available at* http://www.aboutads.info/resource/download/DAA.Commitment.pdf.

[15] *See* Press Release, W3C, *Two Drafts Published by the Tracking Protection Working Group* (Mar. 13, 2012), *available at* http://www.w3.org/News/2012#entry-9389; Press Release, W3C, *W3C Announces First Draft of Standard for Online Privacy* (Nov. 14, 2011), *available at* http://www.w3.org/2011/11/dnt-pr.html.en.

While work remains to be done on Do Not Track, the Commission believes that the developments to date, coupled with legislative proposals, provide the impetus towards an effective implementation of Do Not Track. The advertising industry, through the DAA, has committed to deploy browser-based technologies for consumer control over online tracking, alongside its ubiquitous icon program. The W3C process, thanks in part to the ongoing participation of DAA member companies, has made substantial progress toward specifying a consensus consumer choice system for tracking that is practical and technically feasible.[16] The Commission anticipates continued progress in this area as the DAA members and other key stakeholders continue discussions within the W3C process to work to reach consensus on a Do Not Track system in the coming months.

B. Data Brokers

The Final Report recommends that companies provide consumers with reasonable access to the data maintained about them. The extent of such access should be proportionate to the sensitivity of the data and the nature of its use.

The Final Report addresses the particular importance of consumers' ability to access information that data brokers have about them. Data brokers are companies that collect information, including personal information about consumers, from a wide variety of sources in order to resell such information for a variety of purposes, including verifying an individual's identity, differentiating one consumer's records from another's, marketing products, and

---

[16] A system practical for both businesses and consumers would include, for users who choose to enable Do Not Track, significant controls on the collection and use of tracking data by third parties, with limited exceptions for functions such as security and frequency capping. As noted above, a website's sharing of behavioral information with third parties is not consistent with the context of the consumer's interaction with the website and would be subject to choice. Do Not Track is one way for users to express this choice.

preventing financial fraud. Such entities often have a wealth of information about consumers without interacting directly with them. Data brokers can compile data that can be used to benefit consumers, such as to help authenticate consumers in order to prevent identity theft or provide them with relevant offers and deals for products and services. However, consumers are often unaware of the existence of these entities, as well as the purposes for which they collect and use data.[17]

The Commission has monitored data brokers since the 1990s, hosting workshops, drafting reports, and testifying before Congress about the privacy implications of data brokers' practices.[18] Following a Commission workshop, data brokers created the Individual References Services Group (IRSG), a self-regulatory organization for certain data brokers that set forth principles to restrict availability to certain non-public information.[19] The industry ultimately terminated this organization. Although a series of public breaches – including one involving

---

[17] As noted above, in connection with online tracking, it is generally inconsistent with the context of the interaction for a consumer-facing entity to share the consumer's data with a third party. Accordingly, such transfers of personal information would be subject to choice.

[18] *See, e.g.*, Prepared Statement of the FTC, *Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information*: *Hearing Before the S. Comm. on Banking, Housing, and Urban Affairs*, 109th Cong. (Mar. 10, 2005), *available at* http://www.ftc.gov/os/testimony/050310idtheft.pdf; *see also* FTC Workshop, *The Information Marketplace: Merging & Exchanging Consumer Data* (Mar. 13, 2001), *available at* http://www.ftc.gov/bcp/workshops/infomktplace/index.shtml; FTC Workshop, *Information Flows: The Costs and Benefits to Consumers and Businesses of the Collection and Use of Consumer Information* (June 18, 2003), *available at* http://www.ftc.gov/bcp/workshops/infoflows/030618agenda.shtm.

[19] *See* FTC, *Individual Reference Services, A Report to Congress* (1997), *available at* http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm.

ChoicePoint – led to renewed scrutiny of the practices of data brokers,[20] there have been no meaningful broad-based efforts to implement self-regulation in this area in recent years.

To improve the transparency of the practices of data brokers, the Final Report proposes that data brokers, like all companies, provide consumers with reasonable access to the data they maintain. Because most data brokers are invisible to consumers, however, the Commission makes two additional recommendations as to these entities.

The Commission has long supported legislation that would give access rights to consumers for information held by data brokers.[21] For example, Senator Pryor and Chairman Rockefeller's S.1207 includes provisions to establish a procedure for consumers to access information held by data brokers.[22] The Commission continues to support legislation in this area to improve transparency of the industry's practices.[23]

---

[20] *See* Prepared Statement of the FTC, *Protecting Consumers' Data: Policy Issues Raised by ChoicePoint*: *Hearing before H. Comm. on Energy & Commerce, Subcomm. on Commerce, Trade, and Consumer Protection, Comm. on Energy & Commerce*, 109th Cong. (Mar. 15, 2005), *available at* http://www.ftc.gov/os/2005/03/050315protectingconsumerdata.pdf.

[21] *See, e.g.*, Prepared Statement of the FTC, *Legislative Hearing on H.R. 2221, the Data Accountability and Protection Act, and H.R. 1319, the Informed P2P User Act: Hearing Before the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Trade, and Consumer Protection*, 111th Cong. (May 5, 2009), *available at* http://www.ftc.gov/os/2009/05/P064504peertopeertestimony.pdf.

[22] Data Security and Breach Notification Act of 2011, S. 1207, 112th Congress (2011); *see also* Data Accountability and Trust Act, H.R. 1707, 112th Congress (2011); Data Accountability and Trust Act of 2011, H.R. 1841, 112th Congress (2011).

[23] *See, e.g.*, Prepared Statement of the FTC, *Data Security: Hearing Before the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Manufacturing, and Trade*, 112th Cong. (May 4, 2011), *available at* http://www.ftc.gov/opa/2011/05/pdf/110504datasecurityhouse.pdf; Prepared Statement of the FTC, *Data Security: Hearing Before the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Manufacturing, and Trade*, 112th Cong.(June 15, 2011), *available at* http://www.ftc.gov/os/testimony/110615datasecurityhouse.pdf; Prepared Statement of the FTC,

The Commission also recommends that the data broker industry explore the possibility of creating a centralized website where data brokers could identify themselves to consumers, describe how they collect consumer data, and disclose the types of companies to which they sell the information.[24] The Commission staff intends to discuss with relevant companies how this website could be developed and implemented voluntarily, to increase the transparency and provide consumers with tools to opt out.[25]

III. Other Policy Initiatives

In addition, the Commission holds public workshops and issues reports to examine the implications of new technologies and business practices on consumer privacy. We outline four notable examples below.

First, in February 2012, the Commission released a staff report on mobile applications ("apps") for children.[26] The report found that in virtually all cases, neither app stores nor app developers provide disclosures that tell parents what data apps collect from children, how apps

---

Protecting Consumers in the Modern World: Hearing Before the S. Comm. on Commerce, Science, and Transportation, 112th Cong. (June 29, 2011), *available at* http://www.ftc.gov/os/testimony/110629privacytestimonybrill.pdf.

[24] *See, e.g.*, Tanzina Vega & Edward Wyatt, *U.S. Agency Seeks Tougher Consumer Privacy Rules*, N.Y. TIMES, Mar. 26, 2012, *available at* http://www.nytimes.com/2012/03/27/business/ftc-seeks-privacy-legislation.html?pagewanted=all ("'It's not an unreasonable request to have more transparency among data brokers.'") (quoting Jennifer Barrett Glasgow, Chief Privacy Officer for Acxiom).

[25] The current website of the Direct Marketing Association (DMA) offers an instructive model for such a website. The DMA – which consists of data brokers, retailers, and others – currently offers a service through which consumers can opt out of receiving marketing solicitations via particular channels, such as direct mail, from DMA member companies. *See* DMAChoice, http://www.dmachoice.org/dma/member/home.action.

[26] FTC Staff Report, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (Feb. 2012), *available at* http://www.ftc.gov/opa/2012/02/mobileapps_kids.shtm.

share it, and with whom. The report recommends that all members of the children's app ecosystem – the stores, developers and third parties providing services – should play an active role in providing key information to parents.[27] The report also encourages app developers to provide information about data practices simply and succinctly. The Commission has already reached out to work with industry to provide parents with the information they need, and some industry participants have taken positive steps to improve disclosures going forward.

To discuss how members of the mobile and online ecosystems can best disclose their data practices to consumers, the Commission will host a public workshop later this month.[28] The workshop will address the technological advancements and marketing developments since the FTC first issued its online advertising disclosure guidelines known as "Dot Com Disclosures,"[29] including the advent of smartphones and tablets. The workshop will examine whether and how to revise the Dot Com Disclosures in the current online and mobile advertising environment and will include a specific panel on mobile privacy disclosures.[30]

---

[27] News reports indicate that some companies, like Apple, are already working to limit certain types of data collection via apps. *See, e.g.*, Kim-Mai Cutler, *Amid Privacy Concerns, Apple Has Started Rejecting Apps That Access UDID*, TECHCRUNCH (Mar. 24, 2012), http://techcrunch.com/2012/03/24/apple-udids/.

[28] FTC Workshop, *Dot Com Disclosures* (May 30, 2012), *available at* http://www.ftc.gov/opa/2012/02/dotcom.shtm.

[29] FTC, *Dot Com Disclosures* (2000), *available at* http://www.ftc.gov/os/2000/05/0005dotcomstaffreport.pdf.

[30] In addition to examining mobile disclosures, the Commission continues to examine other privacy and security issues associated with the mobile ecosystem. *See, e.g.*, FTC Workshop, *Paper, Plastic ... or Mobile?: An FTC Workshop on Mobile Payments* (Apr. 26, 2012), *available at* http://www.ftc.gov/bcp/workshops/mobilepayments/.

Second, the FTC hosted a workshop in December 2011 that explored facial recognition technology and the privacy and security implications raised by its increasing use.[31] Facial detection and recognition technology has been adopted in a variety of new contexts, ranging from online social networks to digital signs and mobile apps. Commission staff sought comments on the privacy and security issues raised at the workshop, which it will address in a report in the coming months.

Third, as discussed in the Final Report, the FTC intends to examine the practices of large platforms such as Internet browsers, mobile operating system providers, Internet Service Providers, and large social media platforms that can collect data from numerous sources to build extensive profiles about consumers. Commission staff will host a workshop in the second half of 2012 to examine questions about the scope of such data collection practices, the potential uses of the collected data, and related issues.

Finally, the Commission is undertaking a comprehensive review of the COPPA Rule in light of rapidly evolving technology and changes in the way children use and access the Internet.[32] In September 2011, the Commission proposed modifications to the Rule intended to update the Rule to meet changes in technology, assist operators in their compliance obligations, strengthen protections over children's data, and provide greater oversight of COPPA safe harbor

---

[31] FTC Workshop, *Face Facts: A Forum on Facial Recognition Technology* (Dec. 8, 2011), *available at* http://www.ftc.gov/bcp/workshops/facefacts/.

[32] *See* Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule, 75 Fed. Reg. 17,089 (Apr. 5, 2010), *available at* http://www.ftc.gov/os/fedreg/2010/april/P104503coppa-rule.pdf.

programs.[33] For example, the Commission proposed adding geolocation information and cookies used for behavioral advertising to the definition of "personal information," which would have the effect of requiring parental consent for collection of this information. In addition, the Commission proposed adding a new provision addressing data retention and deletion. The Commission received over 350 comments on its proposed amendments to the COPPA Rule, which are being reviewed by FTC staff.

IV. Enforcement

In addition to its engagement on the policy front, enforcement remains a top priority for the agency. To date, the Commission has brought 36 data security cases; almost 80 cases against companies for improperly calling consumers on the Do Not Call registry;[34] 86 cases against companies for violating the Fair Credit Reporting Act ("FCRA");[35] more than 100 spam and spyware cases; 18 COPPA cases;[36] and numerous cases against companies for violating the FTC Act by making deceptive claims about the privacy and security protections they afford to consumer data. Where the FTC has authority to seek civil penalties, it has aggressively done so. It has obtained $60 million in civil penalties in Do Not Call cases; $21 million in civil penalties under the FCRA; $5.7 million under the CAN-SPAM Act;[37] and $6.6 million under COPPA.

---

[33] The Commission's Notice of Proposed Rulemaking can be found at 76 Fed. Reg. 59,804 (Sept. 15, 2011), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-09-27/pdf/2011-24314.pdf.

[34] 16 C.F.R. Part 310.

[35] 15 U.S.C. §§ 1681e-i.

[36] 15 U.S.C. §§ 6501-6508.

[37] 15 U.S.C. §§ 7701-7713.

Where the Commission does not have authority to seek civil penalties, as in the data security and spyware areas, it has sought such authority from Congress.

Two highly publicized privacy cases – against Google and Facebook – will benefit more than one billion consumers worldwide. The Commission charged Google with deceiving consumers by taking previously private information – the frequent contacts of Gmail users – and making it public in order to generate and populate a new social network, Google Buzz.[38] This, the Commission alleged, was done without the users' consent and in contravention of Google's privacy promises. As part of the Commission's decision and consent order, Google must protect the privacy of consumers who use Gmail as well as Google's many other products and services. Under the order, if Google changes a product or service in a way that makes any data collected from or about consumers more widely available to third parties, it must seek affirmative express consent to such a change. In addition, the order requires Google to implement a comprehensive privacy program and obtain independent privacy audits every other year for the next 20 years.

The FTC's case against Facebook alleged numerous deceptive and unfair practices.[39] These include the 2009 changes made by Facebook so that information users had designated private – such as their "Friends List" or pages that they had "liked" – became public. The complaint also charged that Facebook made inaccurate and misleading disclosures relating to how much information about users' apps operating on the site could access. For example, Facebook told users that the apps on its site would only have access to the information those

---

[38] *Google, Inc.*, Docket No. C-4336 (Oct. 13, 2011) (final decision and consent order), *available at* http://www.ftc.gov/opa/2011/10/buzz.shtm.

[39] *Facebook, Inc.*, Matter No. 0923184 (Nov. 29, 2011) (proposed consent agreement), *available at* http://www.ftc.gov/opa/2011/11/privacysettlement.shtm.

apps "needed to operate." The complaint alleges that in fact, the apps could view nearly all of the users' information, regardless of whether that information was "needed" for the apps' functionality. The Commission further alleged that Facebook made promises that it failed to keep: It told users it would not share information with advertisers, and then it did; and it agreed to make inaccessible the photos and videos of users who had deleted their accounts, and then it did not. Similar to the Google order, the Commission's consent order against Facebook prohibits the company from deceiving consumers with regard to privacy; requires it to obtain users' affirmative express consent before sharing their information in a way that exceeds their privacy settings; and requires it to implement a comprehensive privacy program and obtain outside audits. In addition, Facebook must ensure that it will stop providing access to a user's information after she deletes that information.

Most recently, the Commission announced a settlement with the social network Myspace. The FTC complaint alleged that, despite promising its users that it would not share consumers' personal information with advertisers, Myspace provided advertisers with the "Friend ID" of users who were viewing particular pages on the site. With the Friend ID, the advertiser could locate the user's Myspace personal profile to obtain his or her real name and other personal information. The advertiser could also combine the user's real name and other personal information with additional information to link broader web-browsing activity to a specific named individual. The proposed order prohibits Myspace from misrepresenting the privacy and confidentiality afforded to users' information, and requires Myspace to create a comprehensive privacy program and undergo third-party audits every other year for the next 20 years.

Finally, the Commission continues to make children's privacy a priority, as demonstrated by a recent a settlement with RockYou, the popular social media gaming company.[40] Despite its claims to have reasonable security, RockYou allegedly failed to use reasonable and appropriate security measures to protect consumers' private data, resulting in hackers gaining access to 32 million email addresses and RockYou passwords. In addition, the Commission charged that RockYou collected personal information from approximately 179,000 children it knew to be under 13 without providing notice or obtaining parental consent, as required by COPPA and despite claims to the contrary. Under the Commission's settlement, RockYou must implement a data security program and undergo audits every other year for the next 20 years and pay a $250,000 civil penalty.

V. Education

The FTC conducts outreach to businesses and consumers in the area of consumer privacy. The Commission's well-known OnGuard Online website educates consumers about many online threats to consumer privacy and security, including spam, spyware, phishing, peer-to-peer ("P2P") file sharing, and social networking.[41] Furthermore, the FTC provides consumer education to help consumers better understand the privacy and security implications of new technologies. For example, last year the Commission issued a guide that provides consumers

---

[40] *See United States v. RockYou, Inc.*, No. CV 12 1487 (N.D. Cal. filed Mar. 26, 2012) (consent decree).

[41] *See* www.onguardonline.gov. Since its launch in 2005, OnGuard Online and its Spanish-language counterpart Alerta en Línea have attracted more than 25 million visits.

with information about mobile apps, including what apps are, the types of data they can collect and share, and why some apps collect geolocation information.[42]

The Commission has also issued numerous education materials to help consumers protect themselves from identity theft and to deal with its consequences when it does occur. The FTC has distributed over 3.8 million copies of a victim recovery guide, *Take Charge: Fighting Back Against Identity Theft*, and has recorded over 3.5 million visits to the Web version.[43] In addition, the FTC has developed education resources specifically for children, parents, and teachers to help children stay safe online. The FTC produced the brochure *Net Cetera: Chatting with Kids About Being Online* to give adults practical tips to help children navigate the online world.[44] In less than one year, the Commission distributed more than 7 million copies of *Net Cetera* to schools and communities nationwide.

Business education is also an important priority for the FTC. The Commission seeks to educate businesses by developing and distributing free guidance. For example, the Commission developed a widely-distributed guide to help small and medium-sized businesses implement appropriate data security for the personal information they collect and maintain.[45] The Commission also creates business educational materials on specific topics – such as the privacy

---

[42] *See* Press Release, FTC, *Facts from the FTC: What You Should Know About Mobile Apps* (June 28, 2011), *available at* http://www.ftc.gov/opa/2011/06/mobileapps.shtm.

[43] *See Take Charge: Fighting Back Against Identity Theft*, *available at* http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm.

[44] *See* Press Release, FTC, *OnGuardOnline.gov Off to a Fast Start with Online Child Safety Campaign* (Mar. 31, 2010), *available at* www.ftc.gov/opa/2010/03/netcetera.shtm.

[45] *See Protecting Personal Information: A Guide For Business*, *available at* www.ftc.gov/infosecurity.

and security risks associated with peer-to-peer file-sharing programs and companies' obligations to protect consumer and employee information from these risks[46] and how to properly secure and dispose of information on digital copiers.[47] These publications, as well as other business education materials, are available through the FTC's Business Center website, which averages one million unique visitors each month.[48] The Commission also hosts a Business Center blog,[49] which frequently features consumer privacy and data security topics; presently, approximately 3,500 attorneys and business executives subscribe to these email blog updates.

Another way the Commission seeks to educate businesses by publicizing its complaints and orders and issuing public closing and warning letters. For example, the Commission recently sent warning letters to the marketers of six mobile apps that provide background screening services.[50] The letters state that some of the apps included criminal record histories, which bear on an individual's character and general reputation and are precisely the type of information that is typically used in employment and tenant screening. The FTC warned the apps marketers that, if they have reason to believe the background reports they provide are being used for employment screening, housing, credit, or other similar purposes, they must comply with the FCRA. The Commission made no determination as to whether the companies are

---

[46] *See Peer-to-Peer File Sharing: A Guide for Business*, *available at* http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus46.shtm.

[47] *See* http://business.ftc.gov/documents/bus43-copier-data-security.

[48] *See generally* http://business.ftc.gov/. The Privacy and Data Security portal is the most popular destination for visitors to the Business Center.

[49] *See generally* http://business.ftc.gov/blog.

[50] Press Release, FTC, *FTC Warns Marketers that Mobile Apps May Violate Fair Credit Reporting Act* (Feb. 7, 2012), *available at* http://www.ftc.gov/opa/2012/02/mobileapps.shtm.

violating the FCRA, but encouraged them to review their apps and their policies and procedures to ensure they comply with the Act.

VI. Conclusion

These policy, enforcement, and education efforts demonstrate the Commission's continued commitment to protecting consumers' privacy and security – both online and offline. As noted above, the Commission encourages Congress to develop general privacy legislation and to adopt targeted legislation addressing data brokers. We appreciate the leadership of Chairman Rockefeller and this Committee on these issues and look forward to continuing to work with Congress, the Administration, industry and other critical stakeholders on these issues in the future.