Center for American Progress
Remarks of FTC Commissioner Julie Brill
"Privacy: Tracking our Progress with Pomp and Circumstance"
June 27, 2011

Good morning. It's a pleasure to be here. Thank you to Peter Swire, the Center for American Progress, and Common Sense Media, for inviting me.

Just a couple of weeks ago, we reached the end of the graduation season, a season to which I was particularly attuned this year as my oldest child – or should I say youngest adult? – graduated from high school. But even without that incentive, I always enjoy this time of year, listening to a parade of leaders and celebrities attempting to impart wisdom to graduates distracted by the itchiness of their polyester robes, the fear – probably justified – that their family will take this one last opportunity to embarrass them in front of their peers, and the anticipation of the real celebration that will begin once Grandma and Aunt Mimi are tucked away in their Holiday Inn Express suite.

This season yielded a fine crop of commencement speeches: The president and the first lady were inspiring, as always. Amy Poehler did a nice job at Harvard working the lyrics of Outcast's "Heyah" into some sound advice on learning to rely on others. Former President Clinton mesmerized the crowd at NYU, reaffirming his role as the nation's orator-in-chief. But it was Tom Hanks at Yale, who, for me, captured the Zeitgeist into which we send this year's graduates.

Hanks opened his speech with these words: "Please do <u>not</u> turn off your electronic devices. Leave your iPhone, you iPad, your Sidekicks, your Droids, your blackberries powered up, recording, photographing, texting all that emerges from this stage over the next few minutes.

Later on today, you can compare your Tweets and Facebook comments…to determine whether anything memorable went down. [Then] take this speech, set it to music, maybe insert some crazy-looking graphics; star in the video yourself, post it on the web, and if it becomes a viral sensation, you will be equal to any cat playing with a paper bag, any set of twin toddlers talking gibberish to each other …Such are the possibilities in our brave new world, the world you inherit whether you like it or not."

I was pondering Tom Hanks' characterization of our times as I watched my son graduate. When I was his age, I left home for Princeton, sure I was on the cutting edge of technology with my portable (a mere 20 pounds!) electric typewriter – an IBM Selectric, no less, with the correcting ribbon, and my cool new turntable. My son leaves for UMass Amherst in a few weeks with a cell phone that has more computing power than was available to the entire computer science department at Princeton in my day. And he wants an upgrade!

As President Clinton succinctly put it in his commencement address: "Ten-year-olds can find out things on the Internet that I had to go to university to learn."

When I look at the brave new cyber-world Tom Hanks and Bill Clinton captured so well, I can't help but think of the words of Shakespeare's Miranda: "Oh Wonder! How many goodly creatures are there here!"

Because of innovations in the Internet, social media, mobile communications, and location-based apps, we can now become friends with people whose voices we've never heard. We can reconnect with folks we knew years ago but lost touch with. We can tweet our thoughts to a cyber café full of anyone who wants to listen.

We shop for groceries online – go to the movies online – share photo albums online – pay traffic tickets online – even date online.

Today, we see aid workers delivering prenatal care, AIDs treatments, and vaccinations to the farthest corners of the developing world using mobile phones and online databanks. And we watch as populist movements, armed only with Twitter and the Internet, bring down dictatorships.

Miranda had it right: Oh wonder, indeed.

But, of course, that is not the whole picture. Allow me to quote Tom Hanks one more time: "A sober look shows that just as the world has gotten to be a better place after all, it has also grown a bit worse at the exact same rate – a one step up, one step back sort of cosmic balance between forward progress and cultural retreat."

Just as the Internet and other technological innovations are extending our reach to the limits of our imagination, those providing us with all this are reaching back – harvesting and trading in information about where we are, what we do, who we meet, what we buy. The amount of tracking of an individual's behavior online—what sites she visits, what ads she clicks on, what she says when she chats and where she wanders through the day—is unprecedented. And since it is largely undetected by the consumer, it is an encroachment on consumer privacy – the yin to all of this wondrous cyber yang.

For two decades, the FTC has monitored – and worried about -- the price in terms of privacy that consumers are paying for access to our burgeoning cyberspace. We've worked to preserve consumers' control over their private data as early as the 1990s, when we relied

primarily on a "notice and choice" model, counting on businesses to give consumers clear choices about how their data is used, and counting on consumers to read and understand privacy policies before making those choices.

The theory is sound, but it has proven unworkable. It is not reasonable to expect consumers to read and understand privacy policies – most about as long and as clear as the Code of Hammurabi – especially when all that stands between them and buying a new flat-screen TV, or playing the latest version of Angry Birds, is clicking the little box that says "I consent."

The Commission has also played defense, focusing on privacy violations that cause indisputable harm: data breaches, identity theft, invasions of children's privacy, spam, spyware, and the like. But this approach falls short as well: it only addresses infringements on privacy *after* harm has been done, giving too little incentive to companies to design systems that will not do harm in the first place. Also, by focusing only on tangible harms to consumers, this approach misses the less quantifiable – but none the less real – injuries suffered by those whose sensitive information – about medical conditions, children, or sexual orientation – is exposed.

Furthermore, neither the notice-and-choice model nor the harm-based model speaks to advances in technology that present ever more sophisticated opportunities to collect data – including the ability to gather information about consumers' every move from their smartphones. And ever more sophisticated opportunities to manipulate data – including the ability to take information that has been stripped of personal identification and re-associate it with specific individuals.

This new reality led the FTC staff to prepare a preliminary report proposing a new privacy framework, called "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers."[1]

The report makes three principal recommendations. First, we call for companies to build privacy and security protections into new products, not just retrofit them after problems arise. When designing new products and services, the level of security and privacy protection should be proportionate to the sensitivity of the data used. And companies should limit the amount of information collected to what is needed, and retain it only as long as needed.

Second, we call for privacy policies that consumers can understand -- without having to retain counsel. The report suggests that one way to simplify notice is to exempt what we have called "commonly accepted" practices from the first layers of notice – practices like sharing data with the shipping company that will deliver the product that you just ordered. When these disclosures of obvious uses of data are culled from privacy statements, the consumer can focus on more pertinent uses of her personal information.

And third, we call for companies to be more up front with consumers about how they collect data, how they use it, and how long they keep it. Companies need to share with consumers the profiles they are compiling, especially if these profiles are informing decisions about loans, insurance, employment or other sensitive matters.

[1] Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (2010) (preliminary FTC staff report), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

When taken as a whole, I believe the framework we have proposed is flexible enough to allow businesses and consumers to continue to profit from an innovating, growing, and rich information marketplace, and sturdy enough to provide guideposts on how to continue to innovate, grow, and enrich in a responsible manner.

The Commission's most talked-about recommendation – and the one most relevant to the issues we are discussing today – is the creation of Do Not Track mechanisms to allow consumers meaningful control over how their online behavioral information is used. A majority of the Commission has expressed support for such mechanisms, myself included.

Our proposal is a technology-driven approach that will allow consumers to make persistent choices that travel with them through cyberspace, communicating their tracking preferences to every website they visit. It doesn't have to be all or nothing—consumers can be given refined choices about what information is collected and how it is used, giving consumers more meaningful control over their personal information.

The Commission believes that there are five essential components to a Do Not Track mechanism.

- First, it must be simple for consumers to use.
- Second, it must be effective. Companies must honor the tracking choices consumers make or face enforcement actions.
- Third, the Do Not Track mechanism must apply across companies and technologies. Consumers should not be expected to make tracking choices on a company-by-company basis. This raises the issue, also flagged by staff in our

report, of whether Do Not Track should be extended to the mobile environment. With so much information about consumers exchanged in that space, I believe the answer is yes. This branch of the information superhighway is in desperate need of basic reform: A recent study by the Future of Privacy Forum found that, out of the top 30 paid apps, 22 did not even have a basic privacy policy.

- Fourth, Do Not Track must do more than just prevent the consumer from receiving targeted advertising: it must provide the consumer with an opportunity to stop the collection of information about her online behavior.
- And fifth, the choices consumers make through Do Not Track should be persistent. That is, consumers should not have to reset their preferences every time they clear their cookies or close their browsers.

To its credit, the industry is working on developing Do Not Track mechanisms. I won't go into the technology—Ed Felten, the FTC's chief technologist and noted computer science expert is here to do just that. We brought Ed to the FTC from Princeton, by the way, where he did an admirable job helping my alma mater's computer science department outstrip my son's phone. We knew we needed the sort of high-powered technical expertise Ed and his team bring to the FTC if we were going to meaningfully engage industry in discussions about workable, effective Do Not Track mechanisms that can function in the traditional online environment as well as the mobile space.

I spent last week in Brussels attending a number of different conferences and workshops, including one that focused on online tracking. Two things stood out there. First, there is tremendous momentum internationally for Do Not Track mechanisms. And second, from a

policy perspective, the European Commission is approaching the issue of behavioral advertising in much the same way that we are. Everyone recognizes that behavioral advertising helps support online content and services and that many consumers value the personalization such ads provide. But we are also all concerned that much of the tracking underlying this advertising is invisible to consumers who, at present, do not have real choices about how – or if – their personal information about their cyber behavior is collected and used.

I want to spend a few minutes talking about online privacy and tracking related to children. While we have a responsibility to protect all consumers, that responsibility increases for children.

The FTC enforces the Children's Online Privacy Protection Act, or COPPA, and its implementing rule. COPPA requires operators of certain websites and online services to provide protections in connection with children's information. Interactive websites and online services directed to children under the age of 13, and operators of general audience sites and services having knowledge that they have collected information from children, must comply with COPPA.

The Commission recently announced its largest civil penalty in a COPPA action, a $3 million settlement against Playdom, a leading developer of online multi-player games.[2] We alleged that the company and 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. In addition to the civil penalty, the settlement permanently bars the

[2] **Error! Main Document Only.***See U.S. v. Playdom, Inc.*, No. SACV11-00724 (C.D. Cal. filed May 11, 2011), *available at* http://www.ftc.gov/opa/2011/05/playdom.shtm.

company from violating COPPA and from misrepresenting its information practices regarding children.

The COPPA rule went into effect in 2000. We began a review of the rule last year, five years before we had to, to ensure that the rule continues to work in today's new technological world, especially the rapid expansion of mobile communications.

The review is ongoing, but the public comments we received and the roundtable discussions we held indicate widespread consensus that COPPA and its implementing rule are written broadly enough to encompass most forms of mobile communications. For example, technologies such as interactive mobile applications, games, and social networking services that access the Internet are clearly online services covered by COPPA. There was less consensus, however, as to whether certain mobile communications, such as text messages, are online services that come under the rule. We continue to look closely at this question.

And while COPPA encompasses our responsibility to protect children's privacy online, it doesn't relieve us of the obligation to prepare children to become consumers who will make wise and responsible choices about their online behavior. We are particularly proud of our educational booklet, "Net Cetera: Chatting with Kids About Being Online," which 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.[3] 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. Through our partnership with schools, community groups, and local law

[3] **Error! Main Document Only.** *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.

enforcement, the FTC has distributed more than 7.8 million print copies of the guide over the past couple of years.

I'd like to end today with some thoughts from a Princeton graduate who knows a little bit about the opportunities and perils of cyberspace: Jeff Bezos, founder of Amazon.com and Princeton University's commencement speaker last year. He said: "Tomorrow, in a very real sense, your life – the life you author from scratch on your own – begins…. When you are 80 years old, and in a quiet moment of reflection narrating for only yourself the most personal version of your life story, the telling that will be most compact and meaningful will be the series of choices you have made. In the end, we are our choices."

The FTC's work on privacy and on tracking is all about keeping that inspiring statement true. We want to build a rich online environment where individuals can make meaningful choices about how they present themselves to the world. And that can only come about when individuals control private information about who they talk to, what they say, where they go, and what they do – in cyberspace, the mobile space, and beyond.

Thank you.