

**Remarks of FTC Chairman Jon Leibowitz at
White House Privacy Event
As Prepared for Delivery
February 23, 2012**

What a pleasure to be here to spotlight the efforts of the Administration, Congress, the Federal Trade Commission, consumer groups, and industry to protect consumer privacy online. In so doing, we promote a thriving Internet marketplace that is a cyber-hope of our economy.

At the turn of the century, one genius deployed leading-edge technology and revolutionary sales tactics to transform the American market for consumer goods. Now, before any of the company representatives with us panics that Larry Page is about to get a mention over Bill Gates, or Mark Zuckerberg over Jeff Bezos, the century was last century and the genius was Henry Ford. He said: "It is not the employer who pays the wages. Employers only handle the money. It is the customer who pays the wages."

He was exactly right: It's all about the consumer.

The FTC acknowledged that when we challenged industry to let consumers choose whether they are tracked online. And you – this century's captains of industry – acknowledged it when you stepped up to that challenge. Respecting consumers' privacy and protecting their personal data online encourages trust in Internet commerce, in turn fueling the growth of the cyber-economy and paying all of our wages.

We are honored to stand today with the Administration and the Department of Commerce, which has engaged in extensive study and research that has resulted in a White House Consumer Privacy Bill of Rights Blueprint. And members of Congress on both sides of the aisle and both sides of the Capitol have demonstrated that they understand how important it is that consumers' personal data be treated with care and respect.

Protecting privacy – online and off – is central to the FTC's larger missions: allowing the nation's consumers to confidently navigate the marketplace and ensuring competition as it shapes the economy. We view our missions as a call to action. We've gone after dozens of companies that broke their privacy promises, scores of telemarketers that called consumers whose names were on the Do Not Call registry, and more than a hundred scammers peddling unwanted spam and spyware. Most notably, last year, two of the largest Internet companies entered into consent orders with the FTC that require both to honor their privacy commitments to hundreds of millions of consumers worldwide and to hire outside auditors to monitor their privacy practices.

Since our founding in 1914, the FTC also has had a policy function, which has focused recently on privacy. Just last week, we released a report on mobile apps for children. We found that in virtually all cases, neither app stores nor app developers tell parents what data apps collect from children, how apps share it, and with whom. That has to change. No one has the right to keep parents from taking a firm hold of their child's hand as they cross the information superhighway. We plan to work with industry to make sure that parents get the information they need.

The principles underlying much of our work on privacy are laid out in a December 2010 draft staff report on privacy which, in part, proposed that companies follow three principles when handling personal data. First, they should incorporate privacy protections into products as they are developed – that is, privacy by design. Second, they should offer consumers more choice about how their data is collected and used. And third, they should provide better transparency – that is, information to consumers about how all companies, including personal information brokers, handle private data. We'll release our final report soon.

As part of the draft Privacy Report, we recommended a Do Not Track system that would let consumers choose what information is collected about them online and how it's used. We envisioned a mechanism that would work on all sites; be easy to use; have staying power, even if browsers are updated or cookies deleted; allow consumers to limit how much data is gathered about them online (and not just how many targeted ads they see); and be meaningful – that is, if companies do not honor the choices consumers make through Do Not Track, they will face consequences – no loopholes.

Today we are proud to report that a powerful group of leaders has come together to respond to our call.

For the past several years, the online advertising industry has been working to develop an icon that consumers could click to opt out of receiving targeted ads. Today, although it is still a work in progress, the ad industry has obtained buy-in from companies that deliver 90 percent of online behavioral advertisements; and, with the Better Business Bureau, it has established a mechanism with teeth to address non-compliance, backed up with FTC enforcement. Said differently, if they don't enforce it, we will.

More recently, industry has gone further: it has committed not to release consumers' browsing data for sensitive purposes, such as to employers making hiring decisions or to insurers determining coverage. And it is moving toward simplifying the opt-out page and ensuring that, when consumers do elect not to be tracked, their choice stays with them, regardless of whether they clear their cookies or update their browser.

In a related effort, very early on the companies that make web browsers stepped up to our challenge to give consumers choice about how they are tracked online, sometimes known as the browser header approach. 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. Mozilla introduced a Do Not Track privacy control for its Firefox browser that an impressive number of consumers have adopted; Apple included a similar Do Not Track control in Safari.

Up until now, the advertising industry and the browser vendors have operated on parallel but separate tracks. But today, with the advertising industry announcing that it will honor consumer choices about tracking made through web browser settings, the two initiatives are beginning to come together. As a result, consumers will be able to opt out of tracking through either the icon on advertisements they see or through their browser settings, and America will move further down the road to protecting consumer privacy.

While these developments are encouraging, we still need to ensure that all companies that track users – not just advertisers – are at the table. To that end, the World Wide Web Consortium (W3C), an Internet standards-setting body, gathered engineers, consumer groups, and participants across the broad technology industry to create a universal standard for Do Not Track. We look forward to their deliberations also bearing fruit over the coming year.

Certainly challenges lie ahead. We all understand that there are privacy problems in cyberspace. We spend much of our time as an agency bringing cases against companies that fail to honor their privacy commitments. And the current Do Not Track initiatives are not yet complete. But these problems aside, let's take stock of how far we've come. American business is committed to improving tracking controls and, at a more basic level, to letting consumers choose how their data is handled and shared; that is, to protecting consumer privacy.

Henry Ford once said: "Coming together is a beginning; keeping together is progress; working together is success." With the encouragement of this Administration – which has so keenly recognized the link between protecting consumer privacy online and engendering consumer trust in Internet commerce – an impressive public-private partnership has made a beginning, coming together around one small agency's Do Not Track initiative.

Today we celebrate the progress we have made as we've kept together: Apple, Google and other tech companies announced yesterday they will insist on privacy policies in mobile space. Business has committed to advancing Do Not Track. And the President has reminded the world that, in the United States, personal privacy is a right.

From here we can see success, which will come as long as we continue to work toward one common goal: a thriving, innovative cyber-economy fueled by the confidence of consumers whose privacy and personal data are handled with care and respect.

Thank you.