



Federal Trade Commission

**4A's Transformation 2011 Conference
Austin, Texas**

**A Word From Washington about Behavioral Advertising and Do Not Track
David C. Vladeck¹
Director, FTC Bureau of Consumer Protection
March 8, 2011**

Thank you for inviting me to speak today. It is a pleasure to be here to share my thoughts on behavioral advertising and the FTC's "Do Not Track" proposal.

I'm sure many of you have heard about this proposal and would like to know more about what we have in mind. Let me start by saying that the Commission recognizes that behavioral advertising benefits consumers. It delivers ads relevant to consumers' interests. It helps support (s) T9ET7

¹ The views expressed here are my own and do not necessarily represent the views of the Federal Trade Commission or any Commissioner.

To address these privacy concerns by giving consumers the opportunity to exercise informed choice about tracking, the Commission, consumer groups, and leading industry participants – including many of you here today – have supported improving transparency and consumer choice with regard to tracking. The FTC has envisioned Do Not Track as a one-stop-shop where consumers can exercise a choice not to be tracked, and where marketers would have to respect such their choice.

At the outset, let me put one myth about Do Not Track to rest. Some people think that the FTC believes legislation is necessary to accomplish Do Not Track. That isn't so. To be sure, we've been disappointed in the progress of self-regulation. But at the same time, our hope is that industry will implement a simple, effective, and enforceable Do Not Track system. There has been considerable progress in this regard since we issued our privacy report in December, and we commend these ongoing efforts.

I'd like to talk a bit more about Do Not Track. But let me first highlight some of the FTC's efforts to promote transparency and choice in the online advertising arena. Then, I'd like to discuss some specifics about Do Not Track and what we'd expect from any Do Not Track system.

I. FTC's Efforts

Consumer privacy concerns have received a lot of public attention recently from Congress, the FTC, the Department of Commerce, the FCC, consumer groups, and the media. Privacy is not a new issue for the FTC: it has been one of the Commission's highest consumer protection priorities for more than a decade.

The Commission's goals in the privacy arena have remained constant: to empower consumers to protect their personal information and to ensure that consumers can confidently take advantage of the many benefits offered by the ever-changing marketplace.

We hosted a series of three public roundtables on consumer privacy last year to make sure that our approach to privacy was keeping pace. Based on discussions at the roundtables and the comments received, in December the Commission staff proposed a new framework for protecting consumer privacy in this era of rapid technological change. The report advanced three main concepts, all based on the need to ease the burden on consumers.

² Preliminary FTC Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 1, 2010), <http://ftc.gov/os/2010/12/101201privacyreport.pdf>.

We also review our rules periodically to make sure they are keeping up with the times. For example, we're reviewing our Rule implementing the Children's Online Privacy Protection Act and hope to complete that review this Spring.

In addition to our policy efforts, the Commission has an aggressive privacy enforcement agenda. In the last fifteen years, we have brought 33 cases against companies that failed to implement reasonable security measures to protect consumer data; 64 cases against companies for improperly calling consumers on the Do Not Call registry; 83 cases against companies for violating the Fair Credit Reporting Act; 96 spam cases; 15 spyware cases; and 15 cases against companies for violating the Children's Online Privacy Protection Act. In addition, the Commission has brought numerous cases against companies for violating the FTC Act by making deceptive claims about the privacy of the information they collect, which has the effect of undermining consumer choices on privacy. Let me highlight just a few recent examples.

First, the Commission recently settled a case against EchoMetrix, a company selling a software program called Sentry Parental Controls that enables parents to monitor their children's activities online.³ The Commission alleged that EchoMetrix sold the information that it collected from children to third parties for marketing purposes, without telling parents. The Commission's order prohibits that practice and requires the company to delete any such information from its marketing database.

Second, this past September, the Commission settled a case against US Search, a data broker that maintains an online service that enabled consumers to search for public information

³ See FTC Press Release, "FTC Settles with Company that Failed to Tell Parents that Children's Information Would be Disclosed to Marketers" (Nov. 30, 2010), *available at* <http://www.ftc.gov/opa/2010/11/echometrix.shtm>.

about others.⁴ The company allowed consumers to opt out of having their information appear in the search results, for a fee of \$10. Although 4,000 consumers paid the fee and opted out, their names still appeared in search results. The settlement requires US Search to disclose limitations on its opt-out offer, and to provide refunds to consumers who had previously opted out. The message here is that when consumers choose to take advantage of a company's opt out mechanism, the company must im

⁴ See FTC Press Release, "Online Data Broker Settles FTC Charges Privacy Pledges Were Deceptive: (Sept. 22, 2010), available at <http://www.ftc.gov/opa/2010/09/ussearch.shtm>.

⁵ See FTC Press Release, "Twitter Settles Charges that it Failed to Protect Consumers' Personal Information; Company Will Establish Independently Audited Information Security Program" (June 24, 2010), available at <http://www.ftc.gov/opa/2010/06/twitter.shtm>.

corporation, which had operated a magazine and website directed to gay male youth, but had gone bankrupt.⁶ The question was whether XY's subscriber lists and other highly sensitive information – including names, street addresses, personal photos, and bank account information from gay teens – could be transferred in the bankruptcy proceeding. The letter warned that selling, transferring, or using this information would be inconsistent with the privacy promises made to the subscribers, and may violate the FTC Act. The letter urged that the data be destroyed. Ultimately, the bankruptcy court ordered the destruction of the information.

The thread that ties these cases together is this: The FTC will step in when false or misleading privacy claims have the effect of undermining consumer choices that implicate the privacy of their information.

II. Do Not Track

So let me get back to Do Not Track. Obviously, we're concerned about practices that subvert or undermine consumer choice, and our enforcement agenda reflects that concern. But we want to do more than get rid of bad practices; we w

⁶ Available at <http://www.ftc.gov/os/closings/100712xy.pdf>.

over their online tracking. And of course a coalition of media and marketing associations, including the 4A's, has developed self-regulatory guidelines and an opt-out mechanism for behavioral advertising. The breadth of this coalition effort is promising, demonstrating that a wide range of companies are willing to join in programs designed to offer consumers choice. Most recently, the Interactive Advertising Bureau announced that it has *required* all of its members to adhere to these self-regulatory guidelines. This is an important step forward, because once a company makes a clear commitment to privacy, its failure to honor that commitment can be the basis of an FTC enforcement action. These steps represent positive progress in this area.

I am glad to see industry turning to address this challenge head on, and eager to see the final results. I often get asked the question, "What does self-regulation have to include in order to be satisfactory for the FTC?" "How can we answer the call for Do Not Track, without a legislative mandate?" A successful Do Not Track mechanism could be developed by industry, even without legislation, so long as that mechanism in

mechanism would prevent the tracking of consumers by any means. Because it may be difficult or impossible for consumers to detect violations, to ensure compliance and aid enforcement it is essential that violations can be detected by technological means. The FTC must play an active role in enforcing a self-regulatory Do Not Track mechanism. The Commission can use Section 5 to enforce representations made to consumers, and companies that fail to adhere to these representations need to be referred to the FTC.

Third, a Do Not Track mechanism must be universal. Making consumers exercise choices on a company-by-company or industry-by-industry basis places too much burden on consumers. They should be able to go to one place to exercise their preference across the board. Our call for a “universal” Do Not Track mechanism is often compared to the Do Not Call program. Before the FTC implemented Do Not Call, consumers could request that individual companies stop calling, and both industry and the states offered mechanisms for consumers to express a preference not to be called. The revolution that made Do Not Call such a success was that consumers could register in one place and be done with it.

But that’s where (nis)llj10.680007.001a7116.6801010680010(0)0713266(0)0703200(y)0564016.000 7

Fourth, a Do Not Track mechanism must allow consumers to opt out not only from the *use* of tracked data, but also from its *collection*. Both the collection of information and the serving of behavioral advertising can be of concern to consumers. This is especially true because – at least so far – we don't have a good understanding of wha

the browser visits to signal whether the consumer wants to be tracked or receive targeted ads.

This is one possibility – there likely are others. And here’s where the advantages of self-regulation kick in. I call on industry to use its ingenuity and technical know-how to figure out how to ensure that consumers don’t have to keep making choices over and over again. Or worse, having consumers think they’ve made a choice, and have that choice not be respected.

These five components will help ensure that Do Not Track is designed to make

The recent progress we have seen signals that industry may be headed in the right direction in providing meaningful choice for behavioral advertising through self-regulation. Businesses and industry associations are thinking creatively about ways to improve choice mechanisms for online behavioral advertising. We support those efforts, and encourage you to continue to work aggressively and expeditiously to address this challenge. The Commission hopes that industry will continue to develop tools that meet these criteria, and looks forward to industry innovation in this area. Indeed, the Commission believes that any Do Not Track mechanism should build upon existing industry innovations – and perhaps incorporate elements of the different mechanisms being proposed today – into a comprehensive, effective Do Not Track system that provides consumers with greater transparency and choice – into a comprehens