Federal Trade Commission

4A's Transformation 2011 Conference
Austin, Texas

A Word From Washington about Behavioral Advertising and Do Not Track
David C. Vladeck[1]
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 a diverse range of online content and services that otherwise might not be available, or that consumers would otherwise have to pay for – services such as blogging, social networking and instant access to newspapers and information from around the world. Before you think I am pandering to an audience of advertisers, let me add that behavioral advertising raises serious privacy concerns. Many consumers do not even know they are being tracked. Those who do may be uncomfortable with being tracked, especially if their information may be used for purposes other than serving them ads, but can't figure out what to do about it.

[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:

* First, privacy by design – building privacy and security into companies' procedures, systems, technologies, and business models by design.

* Second, simple consumer choice – streamlining choices for consumers so that they can focus on the choices that really matter to them.

* Third, increased transparency – we need better privacy notices, perhaps in more consistent, shorter, more easily comparable formats.

This proposed framework is intended to inform policymakers as they develop solutions, policies, and potential laws governing privacy. It is also intended to guide and spur industry to develop more robust and effective best practices and self-regulatory guidelines. I urge you to read the Report, which is available on our website.[2] We've received almost four hundred fifty comments on the proposed framework, and after we've reviewed them carefully we expect to issue a final report later this year.

---

[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 implement that choice effectively, regardless of whether the consumer pays to opt out.

Third, this past summer, the Commission alleged that Twitter deceived its customers by failing to honor their choices to designate certain "tweets" as private.[5] On one level, Twitter is a traditional data security case – the FTC charged that serious lapses in the company's data security allowed hackers to obtain unauthorized administrative control of Twitter, including access to private "tweets" and non-public user information. On another level, the case stands for the proposition that social networking services must honor the commitments they make to keep their users' communications private. The order prohibits misrepresentations about the privacy of communications, requires Twitter to maintain reasonable security, and mandates independent, comprehensive audits of Twitter's security practices.

The Commission has taken other measures to ensure that companies keep their privacy promises. For example, last summer, I sent a letter to individuals who had operated XY

---

[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 want to promote good ones. And there is, I hope, common ground about what constitutes good practices. Promoting transparency and giving consumers new ways to exercise choices is a good thing; no one argues that deceiving consumers into surrendering their privacy rights is acceptable. And there's no question that consumers face a daunting burden in the marketplace today to safeguard their privacy. Do Not Track is an important tool to ease that burden.

Industry's efforts since the issuance of our report have been encouraging. For example, major browser developers have recently announced new approaches to give consumers control

---

[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 includes five essential components.

First, a Do Not Track mechanism must be easy for consumers to use and understand. No Do Not Track mechanism will succeed if consumers cannot figure out how to find it and use it. We need simplicity and consistency in the exercise of privacy choices. A Do Not Track mechanism should also make it clear to consumers exactly what they are choosing and if there are limitations to that choice. Industry has a critical role to play here in educating consumers about the choices that it is offering.

Second, a Do Not Track mechanism must be effective and enforceable. While browser-based tools have long existed to block third-party cookies, those tools do not prevent consumers from being tracked by flash cookies or other mechanisms. An effective Do Not Track

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 the similarities between Do Not Call and Do Not Track end. A Do Not Track mechanism must be universal, but it should not be run by the government. Nor should it include a "Registry" of unique identifiers, like telephone numbers. Indeed, there are no persistent identifier for computers. Internet Protocol ("IP") addresses can change frequently. Rather than creating such an identifier, we've recommended that industry develop alternative mechanisms through which consumers could make persistent choices. Browser vendors have suggested ways to implement Do Not Track; ad agencies have suggested other approaches, and joint ad agency/browser efforts might succeed as well. As I said before, I am encouraged by the industry innovation that is taking place in response to our report.

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 what behavioral data is used for, apart from advertising. We asked in our 2009 report on behavioral advertising whether there are secondary uses of behavioral data? Is the fact that I'm buying a deep fryer being shared with my health insurance company? When I visit websites on depression so I can help a friend who is feeling down, will my browsing activity be shared with potential employers? And we've asked this question repeatedly since then. We haven't gotten a clear answer yet. Until we get the answer to our questions about secondary uses, we can't support a Do Not Track mechanism that opts consumers out of targeted advertising but allows data to be used for other purposes.

At the same time, I want to stress that we do not recommend a mechanism that would block all information collection. For example, in our privacy report, we recommend that first-party marketing and fraud detection be permitted as commonly accepted practices. We believe they should also be allowed to collect information on consumers to make sure they're not receiving the same ad 100 times. This is an area where we look forward to reading the comments received. We may need to do better in creating common understandings of the terms "tracking," "collection," and "first party marketing."

Finally, an effective Do Not Track mechanism must ensure that consumers' choices will be persistent. Consumers should not have to reset their preferences every time they clear their cookies or close their browser. One effective method might involve placing a setting on the consumer's browser that would be similar to an opt-out cookie but persistent, so it would not be forgotten when a consumer clears her cookies. That setting would be conveyed to the sites that

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 it as easy as possible for consumers to express their preference whether to be tracked online. We think industry is up to the task of ensuring that both the design and implementation of the mechanisms it is developing will have these components and operate effectively.

III. Conclusion

Let me close by emphasizing again that a Do Not Track mechanism should not undermine the benefits that online behavioral advertising has to offer. Some in the online marketing community say that a Do Not Track system will "destroy" the Internet advertising business because the business depends on tracking consumers covertly. We disagree. We do not believe that an effective Do Not Track mechanism would hurt American businesses. And we do not believe that giving consumers meaningful choice is bad for business.

To the contrary, we have learned that when given the option, many consumers choose to receive some type of tailored advertising rather than opting out entirely. Research confirms that consumers feel more positively towards brands that provide them transparency and control over their data, including the ability to opt out. As industry itself has recognized, providing consumers with choices about online advertising is essential to building the trust necessary for the marketplace to grow. In the long run, mistrust erodes market confidence, and that benefits no one.

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.

Thank you for this opportunity to share my views.