To: Federal Trade Commission
From: Russell Glass, CEO Bizo, Inc.
Date: February 9, 2011
Subject: Response to Request for Comment regarding Online Privacy and Do Not Track.

The FTC's recommendation for Do Not Track (DNT) functionality has been a great lightning rod for industry action, spurring online retailers and the online advertising industry to think hard about the right way to handle delicate privacy issues. However, there are some significant problems with the direction the industry is taking, requiring further clarification and focus from the FTC. I believe that inaction by the FTC to create a course correction could lead to significant consumer and industry harm, and a stifling of high-tech, small business success and innovation in the US, in addition to further monopolistic conditions for Google and Microsoft.

Do Not Track Does NOT Equal Do Not Call

Before diving deeper, let's take a step back and discuss the problems that Do Not Track technology is purportedly trying to solve. Unlike the Do Not Call initiative (which some equate to Do Not Track in a telemarketing context), there is actually significant benefit without undue disruption when there exists safe and anonymous sharing, tracking and online personalization based on consumer interests. In huge numbers, consumers are actively opting to provide some personal information via email, shopping clubs, frequent flier programs, search engines, credit card programs, etc. *in exchange for clear benefit,* whether that benefit be a more personalized experience or to receive discounts and promotions. Thus it is clear that the actual tracking and distribution of information is not the real issue, nor are the technologies that are utilized to track and distribute this information. The problem is that the information being collected and tracked for behavioral targeting online is 1) not always beneficial to the consumer; 2) not always transparent to the consumer; and 3) doesn't always put control in the hands of the consumer. It follows that the solution should be something that allows full transparency and control, and ensures that information is used to benefit consumers. The proposed Do Not Track solution falls short of these goals. Worse yet, it is actually in process of leading the industry in a direction *that prevents* these goals from being achieved. Here are some of the key issues:

Why the Browsers Have a Conflict of Interest

Issue #1: The FTC is putting time pressure on the browser companies to take action, and the browser companies are trying to opportunistically create leverage from the situation to advance their own businesses. As such, they are all rushing solutions to the market without any industry coordination or sufficient consideration for what the right solution might look like for consumers or the market. So we are seeing solutions being shipped that are half-baked, creating consumer confusion, and frankly are not really working to solve the problems at hand. Best case, they are no better than existing solutions and worst case, they literally "break the Web." Browsers have been breaking websites with new releases for years but this is a much more significant change than how basic CSS and scripts are handled – and would have long-

lasting detrimental and unforeseen ramifications to the proper functioning of even the most basic applications online.

Issue #2: The browsers are "conflicted" except for Mozilla, which is the only disinterested party. Microsoft, Google and Apple all have businesses that could benefit significantly from certain implementations of DNT and have too much at stake to deliver solutions that benefit the Web at large and consumers, instead of themselves. For example, if display advertising were to completely fail online, Google would stand to gain significantly as marketing dollars would shift in huge amounts to their leading search engine. As another example, Microsoft owns a large portal and so can force users to enable their domain for targeting while allowing smaller companies to get blocked. These types of activities would be in the best interest of only a few large companies and would be of significant harm to smaller, more innovative companies—ultimately limiting the options available to consumers and harming the market overall. It would be the regulatory equivalent of creating monopolistic conditions online. We've seen the damage this kind of self-interested, unilateral decision-making can do for consumers with Apple's current stance on blocking Adobe's Flash products in the iPhone.

Don't throw the baby out with the bathwater: Cookies make the Web work

Issue #3: The solutions being implemented (Mozilla Firefox being a notable exception) are largely taking a "blunt" approach of blocking third-party cookies. This is the equivalent of preventing the driving of all automobiles because people are sometimes killed in car accidents. There is a significant amount of third-party cookie usage that is critical to the current functioning and well-being of the Web that doesn't harm users in any way. For example, much of the Web's site analytics, ad frequency capping, personalization, fraud verification, "business card" information sharing, and other services require the use of third-party cookies. Simply, the economics and free content and capabilities inherent to the Web have been built on the premise of certain technologies such as third-party cookies. A Microsoft or Google may have an advantage by preventing these other vendors from proliferating, but the consumer would most certainly be harmed by such actions. In my mind, this is one reason that Firefox has taken the approach of using the header solution versus third-party cookie blocking – again being the only "unbiased" party, they are able to look at the solution from a much different perspective. Of course, their solution also has some problems and has the potential to artificially enable the "bad guys" who don't pay attention to the header solution, while harming the "good guys" who do.

A better approach: Transparency and control for consumers, acceptable, enforceable standards for business

In summary, I believe that the FTC has issued an important and valuable call to the industry through its DNT recommendations. I would advise, however, that a follow-up set of recommendations be issued, which will help guide the industry in the right direction:

- Clear consumer benefit, transparency and control should be the primary metrics to measure the success of any DNT solutions.
- The solutions should not break currently accepted methods of transacting online.
- The solutions should recognize that there are multiple uses of the technology and explicitly carve out commonly accepted business practices such as analytics, sharing "Business Card" information and uses for fraud detection.
- Time should be taken to get the *right* solutions to market versus rushing to solutions that may have detrimental long-term ramifications for the benefit of only a few companies.
- The solutions should not artificially enable the "bad guys" who don't follow the regulations, and should act to support the "good guys" who do follow them. Third-party, unbiased organizations such as the Digital Advertising Alliance (DAA) and the Better Business Bureau (BBB) should maintain lists of vendors that are "doing things the right way", and should federate those lists to browsers for default acceptance.
- The only "non-conflicted" party is Mozilla, and I believe the FTC should recommend that Mozilla or other non-profit organizations such as the Digital Advertising Alliance lead the way in creating the right tools that have the interests of the industry and the consumer in mind. By enabling these organizations to take the lead in the implementation of a DNT solution, in collaboration with all of the browser companies, all parties involved (including consumers) will benefit from a more standardized solution that is more widely accepted, understood, and used in the marketplace.

Best,
/rg/
Russell M Glass