15 September 2012

Jon Leibowitz
Chairman
Federal Trade Commission
Washington, DC
(via email)

Dear Chairman Leibowitz,

We are writing to you because of the Federal Trade Commission's (FTC) strong endorsement of efforts by the World Wide Web Consortium (W3C) to reach agreement on a standard for sending a Do Not Track message and for a website's compliance obligations upon receiving that message. While much progress has been made over the last year in moving toward consensus due in part to the FTC's efforts, the W3C's Tracking Protection Working Group appears stalled between two competing proposals, one from industry and the other from privacy advocates. We believe the FTC can help break the impasse between these two proposals.

A clear unified standard for expressing the Do Not Track (DNT) preference and spelling out compliance obligations is necessary to truly protect consumers' online privacy. The W3C process is the best way to achieve that outcome in the near term and the FTC is in unique position to help move the talks to a satisfactory conclusion.

Advocates have already accepted substantial concessions in a good-faith effort to reach an agreement that allows industry to continue a number of practices claimed necessary, while still offering meaningful privacy protections. Let us review some of the key concessions.

First is the issue of whether DNT should limit first-party information collection. Many advocates believe it should. The current W3C consensus, however, is that DNT "on" imposes no obligation on first parties, except that first parties may not help third parties circumvent DNT by sharing data with third parties that they could not themselves collect from DNT "on" users.

Another major concession is sharing data with affiliates. Most advocates believe user expectations should define first parties. The current W3C consensus, however, is that first parties are defined by corporate ownership or affiliation—meaning that the See's Candy website may share its visitors' tracking data with Geico, the insurance company, because both are part of the Berkshire Hathaway corporation. Since many affiliates do not conform to user expectations, allowing affiliates access as if they were part of the first party visited by the user is a substantial concession to industry.

There are two broad areas where industry and advocates remain at loggerheads and where the FTC could help move the discussion forward. The first area of substantial disagreement centers on third-party data collection for "permitted uses." Our focus is on minimizing use of unique ID cookies, device IDs, and other techniques that make tracking easy.

Our compromise proposal would allow "passive collection" of network information (e.g. IP address and User-Agent) subject to retention limits, and "active collection" of other information (e.g. cookies) so long as it cannot be linked to a user or device (e.g. "SeenFordAd=10times" might be allowed, while "Name=JohnSmith" or "UniqueIdentifier=12345" would not). The network information that a third-party website passively collects must be rendered unlinkable upon first processing or in two weeks, whichever comes sooner. If data is unlinkable, it may be

used for any purpose—including advertisement frequency capping and reporting. Our proposal would also permit a third party to collect and retain much more linkable data if it has reason to believe, based on the data it previously collected, that the user is attempting to commit fraud or compromise security. Advocates believe that much of industry has underestimated how much it can do with unlinkable data. We urge the FTC to support the advocates' position.

The second issue is the question of user interface defaults. Advocates believe that all browsers should be free to innovate and compete by designing different UIs and with different default options. After Microsoft announced that Internet Explorer 10 would ship with DNT "on" by default, advocates agreed as a concession that a mainstream browser may not do so and claim compliance with the W3C DNT standard.

A website should not, however, be entitled to ignore a facially valid DNT signal merely because the browser is non-compliant. That approach punishes the user for her choice of browser. After all, even if DNT "on" is the default, it may nevertheless be the user's own choice –as when a user disables and then reenables DNT or if a user chooses the IE10 browser specifically for its privacy-enhancing settings. We urge the FTC to support users by backing our position, especially now that Microsoft has made the DNT setting an explicit choice within the setup flow for Windows 8.

Consumer privacy has suffered in the technical "arms race" between privacy tools and industry tracking practices, and we support efforts to design a consensus approach in hopes of avoiding further undermining of consumer trust online. But the recent news that widely used Apache web server software may be "patched" so that it would by default disregard any DNT signal from an IE 10 browser suggests that the technical arms race may be expanding in scope. We believe that a meaningful DNT standard that browsers enable, users understand and websites honor is the best outcome for all. Strong FTC support for the W3C process would, we hope, nip this damaging "arms race" in the bud.

Meaningful progress will not happen overnight; we understand that industry may need a reasonable period of time to change its data collection practices. Nevertheless, a clear unified standard for expressing the Do Not Track preference and spelling out the compliance obligations is necessary to truly protect consumers' privacy. The W3C talks have reached a point where a clear statement from the FTC will play a decisive role in reaching consensus. Thank you for your consideration.

Sincerely,

Jeff Chester
Center for Digital Democracy

John M. Simpson
Consumer Watchdog

Lee Tien
Electronic Frontier Foundation