Do Not Track and Beyond Workshop Position Paper
John M. Simpson
Privacy Project Director, Consumer Watchdog
Oct. 31, 2012

Consumer Watchdog's Interest In Do Not Track

Consumer Watchdog is known for its success in media advocacy, where our nonprofit, nonpartisan public interest group focuses attention on vital issues of public interest, catalyzing opinion leaders and policymakers. For instance our Privacy Project has helped frame the privacy debate in the media, in Washington, DC, and in the technology industry's hub of California.

Consumer Watchdog was an early advocate of Do Not Track and with good reason. A poll conducted for us in the summer of 2010 by Grove Insight found 80 percent of Americans supported a Do Not Track option managed by the Federal Trade Commission. Eighty-four percent favored preventing online companies from tracking without the user's explicit written consent. Ninety percent supported more laws to protect your personal information. (http://insidegoogle.com/wp-content/uploads/2010/07/MemInternetPrivacy-0727101.pdf)

Consumer Watchdog endorsed U.S. Rep. Jackie Speier's "Do Not Track Me On Line Act", HR 654, and sponsored California Sen. Alan Lowenthal's Do Not Track bill, SB 761. When it became clear that the World Wide Web Consortium's Tracking Protection Working Group offered a genuine possibility of developing a meaningful standard for Do Not Track, specifying how the user's preference would be communicated and what a site's compliance obligations would be, I eagerly joined as an invited expert. Since joining the Working Group a year ago, I believe I have been an active and constructive participant in what I continue to hope will develop a meaningful DNT specification that will benefit both consumers and business.

Goals and Scope of Workshop

When the First Public Working Drafts of the Tracking Preference Expression specification and the Compliance and Scope specification were released, I was impressed with the extent to which the documents relied upon user expectations to develop the language. As the documents have gone through various iterations over the last year, I fear they have too frequently moved away from that guiding principle. For example, what the standard would now consider allowable data sharing amongst affiliates, exceeds what most consumers would expect. Why would you ever expect See's Candy and GEICO insurance to be the same party through corporate affiliation?

Combined with what I perceive to be an ever expanding list of "permitted uses" I think the Working Group is in danger of producing a standard that has no relationship whatsoever to the plain English meaning of Do Not Track. Here is an analogy: Suppose I discover that my neighbor has decided to use a video camera to monitor my bedroom. I find this out because he sends me copies of the video he has taken. I am outraged and ask him to stop tracking my

activities in my bedroom. He agrees, says he has received my do not track message and stops sending me the videos. Nothing else changes.

Exaggerated, perhaps, but I'm trying to make the point that most people believe Do Not Track means exactly that -- do not collect information about my Web browsing activities. Or, in my example analogy, don't record the videos. The gap between what ordinary users will understand DNT to mean and what the standard seems likely to require appears large enough to undermine consumers' trust in the Web. I believe this is a very real problem that must be addressed. At the very least there would need to be considerable education about what the W3C standard means, why it differs from user expectation and how it enhances user privacy. Who will do that? As the W3C DNT standard is emerging, I am hard pressed to understand how DNT gives a user any more protection than blocking third-party cookies and clearing cookies after each browser session.

Another issue that concerns me is the extent to which the Do Not Track issue has been conflated with Online Behavioral Advertising. It doesn't really matter that much to me that I receive ads that are thought to be of interest to me. Indeed, if I knew I was in the market for a particular item, I might well willingly indicate that I was shopping for it so I would see relevant ads. What is troubling are the digital dossiers that are collected and indefinitely maintained about what sites I've visited. Is there a way to determine broad categories into which I might fall, use those for ad targeting, but forgo the digital dossier replete with all the URLs of every site I've ever visited?

Finally, another topic to explore are the privacy concerns that are unique to the mobile market. Admittedly, I have much to learn about this space and its business practices, but I fear the mobile ecosystem is rapidly becoming the Wild West of the Internet.

####