

From: Ryan Schilling
Sent: Monday, November 05, 2007 10:46 PM
To: Behavioral Advertising Comments
Subject: comment for submission

November 5, 2007

Donald S. Clark
Secretary
Federal Trade Commission
Room H-135 (Annex N)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Secretary Clark:

Should Google enjoy the right to track my searches if it chooses until I'm sixty years old in 2038? Should DoubleClick be able to monitor my browsing habits at the sites of its clients without accountability, secure in knowing that neither I nor the majority of Internet citizens have the time to peruse their lengthy and burdensome Privacy Policy? Should companies be able to bury deep within the recesses of their websites mechanisms to "opt-out" of their data collection practices? These are the questions that, as a 14-year veteran user of the Internet, I asked myself when I learned of the coalition of privacy groups who have allied with each other to push for a mandatory "Do Not Track" list online.

The coalition – led by the Consumer Federation of America, the World Privacy Forum (WPF), and the Center for Democracy & Technology (CD&T) – contacted your commission in advance of the "eBehavioral Advertising" workshop you held on November 2-3, 2007, to recommend a series of proactive measures in light of the rapid expansion of Internet advertising. These proposed measures were conceived with the protection of consumers in mind and are based around a set of guiding principles:

- (1) "A consumer's computer belongs to him or her."
- (2) "Buried disclosures do not work."
- (3) "If a distributor puts a program on a computer that the consumer does not want, the consumer should be able to uninstall or disable it."

The privacy coalition's proposed Do Not Track list differs from its spiritual predecessor, the Do Not Call list, in that it would require Internet advertisers to register with the FTC as opposed to having Internet users register. Then, Internet users who wish to amplify their privacy protection could download this list to their machine, so that their browser would automatically opt-out of the registered advertisers' tracking techniques. Having advertisers register is a sensible solution because the nature of the Internet precludes easy end-user registration with the FTC. The IP addresses of Internet users, in contrast with relatively static phone numbers, change frequently as users go online from work, school, home, or via wireless access at their local Starbucks. In addition, IP addresses at home change frequently, for example, when users reboot their modems and receive a new, dynamically generated address from their Internet service provider.

Of equal importance, the coalition recommends that the FTC revisit some old definitions determined in the Network Advertising Initiative (NAI), the agreement that resulted from the FTC's original behavioral advertising workshop in 1999. The NAI specifies that for people to be online, they must be using a computer connected to the web. This underlying concept is today hopelessly outdated. The world changed while the NAI remained static. What this means is that people who connect to the Internet from Blackberries, mobile phones, and PDAs receive no implicit protection from the NAI's guidelines.

This is not to say that the NAI has otherwise been a success. One of the agreement's key tenets is the NAI "Opt-out Cookie." Under this system, a user downloads an NAI cookie to instruct an Internet advertiser not to track his or her online behavior. The WPF rightly argues that from a policy perspective this method was flawed to begin with because downloading a cookie to stop other cookies is by its very nature counterintuitive. The Opt-out Cookie also demands a time commitment from end-users. They must ensure their NAI cookies are kept current as the membership of the association waxes and wanes. All this notwithstanding, there is a general lack of understanding among Internet users about cookies. For example, an InsightExpress study found that of the 59% of respondents who said they had deleted their cookies, only 23% had in fact done so. It seems clear it has been a policy failure to rely on end-users to implement a technological hack that leaves gaping holes in their online privacy.

These gaping holes are not few. The Internet is maturing, as are its marketers. The WPF identified a list of new "persistent identifiers" that Internet advertisers have been employing since the NAI was written: secret cache cookies, Flash cookies, Silverlight Cookies, and XML SuperCookies, and a host of others designed for mobile phones and Blackberries. New methods of reaching consumers are being found in some unexpected places. Canadian researchers were surprised to find a DoubleClick presence in a digital audio book from a public library. In part because the technologies are changing so rapidly, the coalition lastly recommends that regulators require "transparent reporting of industry compliance."

We can view the coalition's proposals and the issue as a whole from a more objective point of view using James O'Toole's *The Executive's Compass*. This book introduces a tool to help understand the constant tensions in a democracy. The compass features Liberty vs. Equality along the North-South axis and Community vs. Efficiency along the East-West axis. O'Toole writes, "these four great themes of political argument are trade-offs with each other, zero-sum positions in which an increment of one value leads to a consequent, equivalent loss of its opposite." The Internet arose out of Community pole of the compass and to a secondary degree the Equality pole. According to O'Toole, Communitarians believe "machines should serve people" not vice versa, and that people should be respected as ends, not as resources in industrial processes." One can still see the lingering spirit of the Internet's original Communitarian and Egalitarian ideals in the movement for Net Neutrality, the continued dominance of free access to most of the Internet, and in sites like Wikipedia where anyone can contribute information to a greater and immensely larger whole.

The influx of corporate interests online over the course of the web's history represents a pull away from its Communitarian roots and toward the Efficiency pole of the Executive's Compass. With so much data being input into their sites, it is only natural that most companies decided to collect it and to find ways to collect more. The WPF notes that "behavioral advertising is lucrative because advertising based on a person's past actions has the potential to result in increased click-throughs and purchases." But in today's unfettered regulatory environment, it is equally natural that many of the Internet's users would wish for the government through the FTC to take on a proactive, regulatory role before the temptation for companies to abuse the data they've collected becomes too great. The tug back toward the Community pole of the Executive's Compass is getting stronger and more organized with each passing day.

For all consumers know, one of the new millennium's brightest corporate stars, Google, may have submitted to temptation already. Google announced in July of 2007 that it was revising its policy of installing a 30-year cookie on all its users' computers. The new Google cookies will be set to expire instead in two years. It is somewhat heartening that Google changed its policy voluntarily, but the fact remains that the Internet giant could reverse this decision tomorrow and would face no ramifications from regulators. Meanwhile cynics and critics maintain the move is nothing but a public relations stunt. Google will easily be able to continue linking the personal ID in the new shorter-lived cookie to previous IDs based on personal information mined from users' searches and browser behavior, creating a lengthy, historical profile on its users.

The Google Toolbar is more insidious than its cookies. The application finds a home on literally millions of computers worldwide in part because it comes coupled with numerous software downloads. The Toolbar allows the user to submit a Google search without first going to the Google homepage. However, when

users activate the program's advanced features, an option that is presented by default during installation, the Toolbar sends data to Google on every page the user visits. The Toolbar also updates itself to new versions without notifying the user, meaning that the application's privacy settings could change without the user's knowledge or consent.

It's important to note that we know precious little about what companies like Google do with the information they collect. All it would take is one scandal, one clear and blatant breach by a major Internet company of consumers' trust, to shake the public's confidence in their privacy online and negatively impact Internet businesses, regardless of their association with the offender. Such a scandal would also result in an outpouring of support for new regulations against Internet companies' ability to collect data, a pull toward Community, toward protection of privacy rights, and away from the Efficiency pole of O'Toole's Executive Compass. I applaud the FTC's decision to run a second workshop on behavioral advertising before such an adversarial environment arises, because a state of objectivity and composure is the most ideal for analyzing this issue. I formally register my support for the objections and proposals raised in the "Do Not Track" coalition's studies, and I hope the FTC initiates further investigation into the burgeoning field of behavioral advertising with the issues they raise in mind.

I sincerely thank you for your time.

Ryan D. Schilling
CO