'Do not track' browser push at odds with online advertisers

August 2 2012, By Robert Channick

When Microsoft unveils a new version of its Web browser, users will be able to traverse the Web like always but with one significant difference: The company plans to make "do not track" the default setting.

That means Internet Explorer 10 will automatically curtail a trove of personal information garnered while users surf anything from cat videos to mommy blogs, data shared by third-party companies to serve up targeted advertising. The move puts Microsoft out in front of a process to set new Internet privacy standards and puts it at odds with the $31 billion online advertising industry.

"Targeted advertising sells for 2 1/2 times as much as nontargeted advertising. It's very effective," said Mike Zaneis, senior vice president and general counsel for the Interactive Advertising Bureau. "When a browser like Microsoft comes in and sets (do not track) by default, they just gave everybody a 60 percent off coupon for our product. We can't survive in that world."

Facing increasing pressure to get ahead of potentially more restrictive legislation, the industry has been struggling to reach consensus for an online privacy standard. In 2011, the World Wide Web Consortium, which sets Internet protocols, put together a working group consisting of companies, privacy advocates and experts that met for the fifth time in June at Microsoft Corp.'s headquarters in Bellevue, Wash.

Some participants said the group should be able to hammer out a

standard privacy policy by the end of the year, but schisms remain. One thing that most agree upon is that making "do not track" a default setting will not be part of their final recommendations. Microsoft's proposed default setting bucks slowly building momentum for an "opt-out" solution.

"It seems clear to me that the Microsoft position, while it may be more protective of consumer privacy, is not a consensus position within the industry," said Federal Trade Commission Chairman Jon Leibowitz.

"Do not track" follows the trail blazed by "do not call," the 2003 federal law that empowered the FTC to create a national registry for consumers to opt out of unsolicited telemarketing calls. The FTC is calling on the digital industry to take a number of online privacy measures, including a "do not track" option.

"The marketplace needs to decide this, and we're letting them," Leibowitz said. "We have not proffered a proposal, other than calling for a 'do not track' option that would be an opt out with limits on collection, with certain exceptions."

Efforts to develop an online privacy standard have failed to keep pace with the technology itself, which has fueled explosive growth in tracking and targeting Web users with "interest-based" advertising.

A report issued in June by Krux Digital showed data collection was up 400 percent year over year, with an average of 50 collection events per page view. Much of that growth comes from online media exchanges, which use real-time bidding platforms to sell targeted ads to individual Web users. Real-time bidding, a segment that barely existed three years ago, is on pace to represent more than a quarter of all U.S. digital display advertising spending by 2015, said Gordon McLeod, president of Krux, a 2-year-old data management company.

Targeted advertising commands a higher price and, some would argue, provides a more satisfying experience for consumers, who receive product offers they might actually be interested in.

"What a consumer benefits from with having their behavior followed is having things that are relevant to them coming up in their advertising experience," said Jason Wadler, executive vice president of Evanston, Ill.-based Leapfrog Online, a direct response marketing company. "If you don't have the ability to target an individual or target a consumer segment, then you are going to see just a whole bunch of random ads that you don't care about, and that's not a good experience."

Tracking has nonetheless raised concern among privacy advocates and regulators that perhaps too much information is being shared without consumer consent.

"This is how we buy our financial products, this is how we search health information, this is how our kids contact their friends," said Jeffrey Chester, a member of the industry group studying the issue and executive director of the Center for Digital Democracy, which focuses on consumer protection and privacy issues. "Companies are able to identify you by race, by income, by health concerns. There's a lot of sensitive data out there that an individual should have more control of. Right now, an individual has no control."

A majority of Web users disapprove of their personal information being collected for targeted advertising. A Pew Internet study released in March found that 68 percent of all Internet users were opposed to targeted advertising because they didn't want their online behavior tracked and analyzed.

The same study showed that just 38 percent of users knew how to limit online data collection. Given the hodgepodge of existing solutions, that is

not surprising.

The Digital Advertising Alliance, a consortium of trade groups, launched its own opt-out program two years ago, a circuitous journey that starts with a small triangular ad choices icon that marketers can embed in their ads. Clicking leads users to a notice page written by the third-party company serving the ad. Within that page is a link to a consumer opt-out site, where users can tell up to 108 participating advertising companies to stop tracking and targeting them. More than 2 million users have opted out to date, Zaneis said.

Flagging "do not track" on a Web browser might be a simpler way to deliver the message to all advertisers, but compliance remains voluntary at this point. The three leading browsers - Internet Explorer, Mozilla's Firefox and Google's Chrome - all offer users an opt-out for tracking.

"Right now, ("do not track") flags mean nothing, because there's no definition for what 'do not track' means," Zaneis said.

While some industry observers believe Microsoft will reverse its position, a company spokeswoman said last week that "do not track" was still on track as a default setting when the new Explorer makes its expected debut this fall.

"By enabling the 'do not track' feature as the default setting in Internet Explorer 10, we're providing our customers more control over how their online behavior is tracked, shared and used," the spokeswoman said.

Analysts see the decision as a shrewd way for Microsoft to appeal to privacy-conscious consumers and take a bite out of rivals such as Google's Chrome browser, which has grown quickly and has about 20 percent of the market. That compares with Internet Explorer's 54 percent, according to NetMarketshare.com. Google, an advertising-

reliant company, has more to lose in a nontracking environment.

Because Microsoft is likely going beyond the forthcoming industry privacy standard, advertisers will have no obligation to honor the default setting for IE 10 users since it will be "noncompliant," Zaneis said. Privacy experts say they would fight such a move.

The debate over "do not track" methodology may not be fully settled until legislation supplants industry self-regulation. With technology continuing to race ahead of policy deliberations, privacy issues may be more complex going forward.

"Technology is way ahead of much of the public debate about what's appropriate and necessary," McLeod said.

(c)2012 Chicago Tribune
Distributed by MCT Information Services

Citation: 'Do not track' browser push at odds with online advertisers (2012, August 2) retrieved 23 April 2024 from https://phys.org/news/2012-08-track-browser-odds-online-advertisers.html