THE WALL STREET JOURNAL.
WSJ.com

WHAT THEY KNOW | AUGUST 2, 2010

Microsoft Quashed Effort to Boost Online Privacy

By NICK WINGFIELD

The online habits of most people who use the world's dominant Web browser are an open book to advertisers. That wasn't the plan at first.

In early 2008, Microsoft Corp.'s product planners for the Internet Explorer 8.0 browser intended to give users a simple, effective way to avoid being tracked online. They wanted to design the software to automatically thwart common tracking tools, unless a user deliberately switched to settings affording less privacy.

That triggered heated debate inside Microsoft. As the leading maker of Web browsers, the gateway software to the Internet, Microsoft must balance conflicting interests: helping people surf the Web with its browser to keep their mouse clicks private, and helping advertisers who want to see those clicks.

In the end, the product planners lost a key part of the debate. The winners: executives who argued that giving automatic privacy to consumers would make it tougher for Microsoft to profit from selling online ads. Microsoft built its browser so that users must deliberately turn on privacy settings every time they start up the software.

Microsoft's original privacy plans for the new Explorer were "industry-leading" and technically superior to privacy features in earlier browsers, says Simon Davies, a privacy-rights advocate in the U.K. whom Microsoft consulted while forming its browser privacy plans. Most users of the final product aren't even aware its privacy settings are available, he says. "That's where the disappointment lies."

Microsoft General Counsel Brad Smith says that in developing the new browsers, the company tried to "synthesize" both points of view about privacy "in a way that advanced both the privacy interests of consumers and the critical role advertising plays in content."

A new report in the Wall Street Journal's "What They Know" series illustrates how companies like Microsoft must balance conflicting interests: helping people surf the Web with its browser to keep their mouse clicks private, and helping advertisers who want to see those clicks. WSJ's Julia Angwin, Nick Wingfield, and Jessica Vascellaro join host Simon Constable as panelists on this special Digits live show.

Microsoft's decision reveals the economic forces driving the spread of online tracking of individuals. A Wall Street Journal investigation of the practice showed tracking to be pervasive and ever-more intrusive: The 50 most-popular U.S. websites, including four run by Microsoft, installed an average of 64 pieces of tracking technology each onto a test computer.

As online advertising grows more sophisticated, companies playing prominent roles in consumers' online experiences have discovered they have access to a valuable trove of information. In addition to Microsoft, such companies include search-engine giant Google Inc., iPhone maker Apple Inc., and Adobe Systems Inc., whose Flash software makes much of the Internet's video, gaming and animation possible. These companies now have a big say in how much information can be collected about individual users.

Many also have big stakes in online advertising. Microsoft bought aQuantive, a Web-ad firm, in 2007 for more than $6 billion, to build a business selling ads online. Google, already a giant in online marketing, in September 2008 launched a Web browser, Chrome, that gives it new insight into Internet users' habits. Apple has launched an ad network, iAds, for its iPhone and iPad. And Adobe last year paid $1.8 billion to buy Omniture, which measures the effectiveness of online ads.

Executives in Microsoft's new ad business were upset when the designers of Internet Explorer hatched the plan to block tracking activity, say people involved in the debate. At a meeting in the spring of 2008, Brian McAndrews, a Microsoft senior vice president who had been chief executive of aQuantive before Microsoft acquired it, complained to the browser planners. Their privacy plan, he argued, would disrupt the selling of Web ads by Microsoft and other companies, these people say.

Kevin P. Casey

Former Microsoft executive Brian McAndrews, who complained about a proposed privacy plan

Mr. McAndrews was taken aback that Explorer planners seemed unwilling to accept input from advertising executives, given that Microsoft had spent $6 billion on a Web-ad firm, according two people who participated in the meeting.

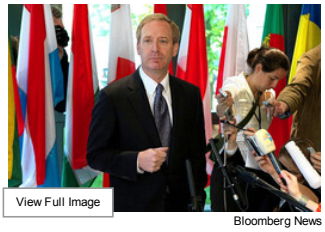
Mr. Smith, the general counsel, says Microsoft weighed both sides of the argument in its debate. He says the company was concerned about the effect strict privacy features might have on free sites supported by advertising, including newspaper sites. Such sites, including WSJ.com, use information derived from tracking to sell targeted ads, an important revenue source.

Web browsers like Internet Explorer can play an important role in protecting privacy because the software sits between consumers and the array of technologies used to track them online. The best-known of those technologies are browser "cookies," small files stored on users' computers that act as identification tags for them when they visit websites.

Some cookies, such as those installed when a user asks a favorite website to remember his password, don't do tracking.

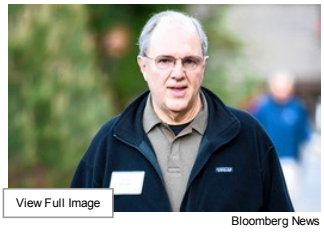
Others are installed on computers by companies that provide advertising services to the websites a user visits. These "third-party" cookies can be designed to track a user's online activities over time, building a database of personal interests and other details.

The Journal's examination of the top 50 most popular U.S. websites showed that Microsoft



Bloomberg News

Microsoft General Counsel Brad Smith (above) and chief research and strategy officer Craig Mundie (below) refereed the debate



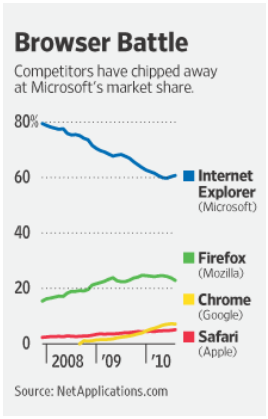
Bloomberg News

Craig Mundie

Michael Rubottom

Interactive Advertising Bureau CEO Randall Rothenberg.

It's rarely a coincidence when you see Web ads for products that match your interests. WSJ's Christina Tsuei explains how advertisers use cookies to track your online habits.



placed third-party tracking devices on 27 of the top 46 sites that it doesn't itself own.

All the latest Web browsers, including Internet Explorer, let consumers turn on a feature that prevents third-party browser cookies from being installed on their computers. But those settings aren't always easy to find. Only one major browser, Apple's Safari, is preset to block all third-party cookies, in the interest of user privacy.

"Only browser developers have the resources and large user bases necessary to create a privacy-friendly version of the Web," says Peter Eckersley, staff technologist with the Electronic Frontier Foundation, a digital-rights advocacy group.

Because Internet Explorer is used by so many people—nearly 60% of all Web users—the 2008 decision by planners of the new version to make it easy for users to block tracking could have had a big effect on the marketplace.

At the time, the practice of tailoring ads to consumers based on their browsing habits was taking off. Google was in the process of buying DoubleClick Inc., a leader in the placing and tracking of online ads, for $3.1 billion. A coalition of privacy groups was petitioning the Federal Trade Commission to develop stricter policies for preventing advertisers from tracking Web-browsing habits. Companies with stakes in Internet advertising were feeling heat to try to stave off government regulation by voluntarily protecting consumer privacy.

Microsoft also was trying to stem the erosion of its browser market share. Internet Explorer, which once had more than 95% of the market, hadn't kept up with competitors. Firefox, a Web browser overseen by the nonprofit Mozilla Foundation, picked up more than 18% of the market by May 2008, helping knock Explorer to 76%, according to NetApplications.com, which tracks browser use.

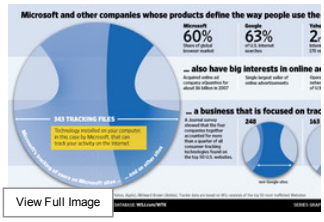
The browser planners at Microsoft believed aggressive new privacy features could help differentiate the new Internet Explorer from rivals, according to several current and former Microsoft executives.

The planners, led by Microsoft veteran Dean Hachamovitch, came up with a concept for preventing consumer tracking. A new feature would monitor where each piece of content on a visited Web page was originating on the Internet—every picture, video or chunk of text. The feature would pay special attention to content from "third party" Internet addresses—addresses different from the one a user sees in the address bar at the top of the browser.

Some of that third-party content could be innocuous things like YouTube video clips displayed on the Web page, which viewers presumably wouldn't want to block. Other items might be tracking tools such as Web "beacons," snippets of code embedded in the page that can monitor the clicks of visitors, or even record their keystrokes. Users might want such tracking tools blocked automatically.

The Internet Explorer planners proposed a feature that would block any third-party content that turned up on more than 10 visited websites, figuring that anything so pervasive was likely to be a tracking tool. This, they believed, was a more comprehensive approach to privacy than simply turning off browser cookies, one that would thwart other tracking methods.

The group also planned to design the Internet Explorer set-up process so that it guaranteed the privacy feature would be used by most people.



View Full Image

When he heard of the ideas, Mr. McAndrews, the executive involved with Microsoft's Internet advertising business, was angry, according to several people familiar with the matter. Mr. McAndrews feared the Explorer group's privacy plans would dramatically reduce the effectiveness of online advertising by curbing the data that could be collected about consumers.

He heard about the proposal through back channels rather than directly from the browser planners, these people say, which surprised him given its implications. Some people who worked in the browser group acknowledge that they should have been more upfront about their intentions. Mr. McAndrews later left the company.

"We were worried it was going to cause a stampede" away from tracking technologies, says an executive who worked with Mr. McAndrews. "It was an act with the potential to reverberate across the industry."

The browser group and its manager, Mr. Hachamovitch, tried to hold their ground. They were reluctant to let advertising executives interfere with the new Explorer design, according to people involved in the debate. Microsoft said that Mr. Hachamovitch and other members of the planning group wouldn't comment on the matter.

The debate widened after executives from Microsoft's advertising team informed outside advertising and online-publishing groups of Microsoft's privacy plans for Explorer. Microsoft Chief Executive Steve Ballmer assigned two senior executives, chief research and strategy officer Craig Mundie and the general counsel, Mr. Smith, to help referee the debate, according to Peter Cullen, Microsoft's chief privacy strategist.

The two men convened a four-hour meeting in Mr. Mundie's conference room in late spring 2008 to allow outside organizations to voice their concerns, including the Interactive Advertising Bureau, the Online Publishers' Association and the American Association of Advertising Agencies.

One of the attendees, Interactive Advertising Bureau Chief Executive Randall Rothenberg, says he was worried that Explorer's proposed privacy features would block not just the collection of consumer data, but also the delivery of some Web advertisements themselves. He says the features "seemed to equate the delivery of advertisements with privacy violations." He was especially troubled, he says, by the prospect of Microsoft turning the features on for all consumers, by default.

One other consideration: Some Microsoft executives were concerned that the preset-privacy plan might jeopardize support among ad-industry organizations that Microsoft wanted to rally against a proposed advertising deal between Google and Yahoo Inc., says a former Microsoft executive. A Microsoft spokeswoman declined to comment on that issue. U.S. regulators ended up blocking the deal.

The former Microsoft executive says he had never before experienced a debate at Microsoft "so driven by external influences and conflicting priorities to protect users" as the tussle over the Explorer privacy controls.

Journal Community DISCUSS

I wish Microsoft had made this the default in IE8, but this article seems to put a lot more blame on Microsoft than other browser makers.

—Bryan MacDonald

"It was a healthy debate," says Mr. Smith, the general counsel, with "well-informed views by people who are passionate."

When Microsoft released the browser in its final form in March 2009, the privacy features were a lot different from what its planners had envisioned. Internet Explorer required the consumer to turn on the feature that blocks tracking by websites, called InPrivate Filtering. It wasn't activated automatically.

What's more, even if consumers turn the feature on, Microsoft designed the browser so InPrivate Filtering doesn't stay on permanently. Users must activate the privacy setting every time they start up the browser.

Microsoft dropped another proposed feature, known as InPrivate Subscriptions, that would have let users further conceal their online browsing habits, by automatically blocking Web addresses suspected of consumer tracking if those addresses appeared on "black lists" compiled by privacy groups.

Mr. Cullen, Microsoft's chief privacy strategist, says the input of outsiders helped Microsoft strike a balance between privacy and advertising interests. The browser, he says, "was a better product than when it came off the drawing-room floor of the Internet Explorer group."

Advertising groups say they were pleased, too. "They ended up with something pretty excellent," says Mr. Rothenberg of the Interactive Advertising Bureau.

Write to Nick Wingfield at nick.wingfield@wsj.com

- **How to Use Microsoft's InPrivate Filtering**
- **The Web's New Gold Mine: Your Secrets**
- **Top Sites Feed Personal Data**
- **How to Avoid Prying Eyes**
- **What They Know About You**
- **Analyzing What You Have Typed**
- **Decoding the Trackers: A Glossary**
- **The Journal's Methodology**