THE WALL STREET JOURNAL.
WSJ.com

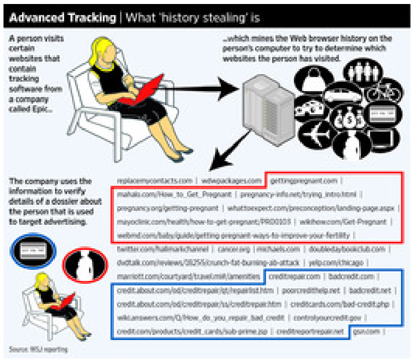
WHAT THEY KNOW | Updated August 19, 2011, 5:19 p.m. ET

Latest in Web Tracking: Stealthy 'Supercookies'

By JULIA ANGWIN

Major websites such as MSN.com and Hulu.com have been tracking people's online activities using powerful new methods that are almost impossible for computer users to detect, new research shows.

What 'History Stealing' Is

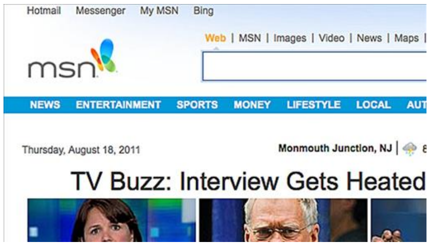

Advanced Tracking | What 'history stealing' is
A person visits certain websites that contain tracking software from a company called Epic...
...which mines the Web browser history on the person's computer to try to determine which websites the person has visited.
The company uses the information to verify details of a dossier about the person that is used to target advertising.
replacemycontacts.com | wdwpackages.com | gettingpregnant.com |
mahalo.com/How_to_Get_Pregnant | pregnancy-info.net/trying_intro.html |
pregnancy.org/getting-pregnant | whattoexpect.com/preconception/landing-page.aspx |
mayoclinic.com/health/how-to-get-pregnant/PR00103 | wikihow.com/Get-Pregnant |
webmd.com/baby/guide/getting-pregnant-ways-to-improve-your-fertility |
twitter.com/hallmarkchannel | cancer.org | michaels.com | doubledaybookclub.com |
dietalk.com/reviews/38255/crunch-fat-burning-ab-attack | yelp.com/chicago |
marriott.com/courtyard/travel.mi#/amenities | creditrepair.com | badcredit.com |
credit.about.com/od/creditrepair/qt/repairlist.htm | poorcredithelp.net | badcredit.net |
credit.about.com/od/creditrepair/ss/creditrepair.htm | creditcards.com/bad-credit.php |
wiki.answers.com/Q/How_do_you_repair_bad_credit | controlyourcredit.gov |
credit.com/products/credit_cards/sub-prime.jsp | creditreportrepair.net | gsn.com |
Source: WSJ reporting

The new techniques, which are legal, reach beyond the traditional "cookie," a small file that websites routinely install on users' computers to help track their activities online. Hulu and MSN were installing files known as "supercookies," which are capable of re-creating users' profiles after people deleted regular cookies, according to researchers at Stanford University and University of California at Berkeley.

Websites and advertisers have faced strong criticism for collecting and selling personal data about computer users without their knowledge, and a half-dozen privacy bills have been introduced on Capitol Hill this year.

Many of the companies found to be using the new techniques say the tracking was inadvertent and they stopped it after being contacted by the researchers.

Mike Hintze, associate general counsel at MSN parent company Microsoft Corp., said that when the supercookie "was brought to our attention, we were alarmed. It was inconsistent with our intent and our policy." He said the company removed the computer code, which had been created by Microsoft.


Hotmail Messenger My MSN Bing
Web | MSN | Images | Video | News | Maps |
msn
NEWS ENTERTAINMENT SPORTS MONEY LIFESTYLE LOCAL AU
Thursday, August 18, 2011
Monmouth Junction, NJ
TV Buzz: Interview Gets Heated

WSJ's Jennifer Valentino-DeVries reports so-called 'supercookies' reside in web sites that are tracking web users' activities and can continue to track users after they click a box to remove cookies from their computer. Photo: Wall Street Journal

Linda A. Cicero/Stanford News Service

Stanford researcher and doctoral candidate Jonathan Mayer

Hulu posted a statement online saying it "acted immediately to investigate and address" the issues identified by researchers. It declined to comment further.

The spread of advanced tracking techniques shows how quickly data-tracking companies are adapting their techniques. When The Wall Street Journal examined tracking tools on major websites last year, most of these more aggressive techniques were not in wide use.

But as consumers become savvier about protecting their privacy online, the new techniques appear to be gaining ground.

Stanford researcher Jonathan Mayer, a Stanford Ph.D. candidate, identified what is known as a "history stealing" tracking service on Flixster.com, a social-networking service for movie fans recently acquired by Time Warner Inc., and on Charter Communications Inc.'s Charter.net.

Such tracking peers into people's Web-browsing histories to see if they previously had visited any of more than 1,500 websites, including ones dealing with fertility problems, menopause and credit repair, the researchers said. History stealing has been identified on other sites in recent years, but rarely at that scale.

Mr. Mayer determined that the history stealing on those two sites was being done by Epic Media Group, a New York digital-marketing company. Charter and Flixster said they didn't have a direct relationship with Epic, but as is common in online advertising, Epic's tracking service was installed by advertisers.

Don Mathis, chief executive of Epic, says his company was inadvertently using the technology and no longer uses it. He said the information was used only to verify the accuracy of data that it had bought from other vendors.

Both Flixster and Charter say they were unaware of Epic's activities and have since removed all Epic technology from their sites. Charter did the same last year with a different vendor doing history stealing on a smaller scale.

Gathering information about Web-browsing history can offer valuable clues about people's interests, concerns or household finances. Someone researching a disease online, for example, might be thought to have the illness, or at least to be worried about it.

More on Internet Privacy

Digits: Questions About Self-Regulation

The Web's New Gold Mine: Your Secrets 7/30/2010

The Web's Cutting Edge, Anonymity in Name Only 8/4/2010

On the Web, Children Face Intensive Tracking 9/17/2010

'Scrapers' Dig Deep for Data on Web 10/12/2010

A Web Pioneer Profiles Users by Name 10/25/2010

Shunned Profiling Technology on the Verge of Comeback 11/24/2010

Complete Coverage: What They Know

The potential for privacy legislation in Washington has driven the online-ad industry to establish its own rules, which it says are designed to alert computer users of tracking and offer them ways to limit the use of such data by advertisers.

Under the self-imposed guidelines, collecting health and financial data about individuals is permissible as long as the data don't contain financial-account numbers, Social Security numbers, pharmaceutical prescriptions or medical records. But using techniques such as history stealing and supercookies "to negate consumer choices" about privacy violates the guidelines, says Lee Peeler, executive vice president of the Council of Better Business Bureaus, one of several groups enforcing the rules.

Until now, the council "has been trying to push companies into the program, not kick them out," Mr. Peeler says. "You can expect to see more formal public enforcement soon."

Last year, the online-ad industry launched a program to label ads that are sent to computer users based on tracking data. The goal is to provide users a place to click in the ad itself that would let them opt out of receiving such targeted ads. (It doesn't turn off tracking altogether.) The program has been slow to catch on, new findings indicate.

The industry has estimated that nearly 80% of online display ads are based on tracking data. Mr. Mayer, along with researchers Jovanni Hernandez and Akshay Jagadeesh of Stanford's Computer Science Security Lab, found that only 9% of the ads they examined on the 500 most popular websites—62 out of 627 ads—contained the label. They looked at standard-size display ads placed by third parties between Aug. 4 and 11.

The industry says self-regulation is working. Peter Kosmala, managing director of the Digital Advertising Alliance, says the labeling program has made "tremendous progress."

Mr. Mayer discovered that several Microsoft-owned websites, including MSN.com and Microsoft.com, were using supercookies.

Supercookies are stored in different places than regular cookies, such as within the Web browser's "cache" of previously visited websites, which is where the Microsoft ones were located. Privacy-conscious users who know how to find and delete regular cookies might have trouble locating supercookies.

Mr. Mayer also found supercookies on Microsoft's advertising network, which places ads for other companies across the Internet. As a result, people could have had the supercookie installed on their machines without visiting Microsoft websites directly. Even if they deleted regular cookies, information about their Web-browsing could have been retained by Microsoft.

Microsoft's Mr. Hintze said that the company removed the code after being contacted by Mr. Mayer, and that Microsoft is still trying to figure out why the code was created. A spokeswoman said the data gathered by the supercookie were used only by Microsoft and weren't shared with outside companies.

Separately last month, researchers at the University of California at Berkeley, led by law professor Chris Hoofnagle, found supercookie techniques used by dozens of sites. One of them, Hulu, was storing tracking coding in files related to Adobe Systems Inc.'s widely used Flash software, which enables many of the videos found online, the researchers said in a report. Hulu is owned by NBC Universal, Walt Disney Co. and News Corp., owner of The Wall Street Journal.

Hulu was one of several companies that entered into a $2.4 million class-action settlement last year related to the use of Flash cookies to circumvent users who tried to delete their regular cookies.

The Berkeley researchers also found that Hulu's website contained code from Kissmetrics, a company that analyzes website-traffic data. Kissmetrics was inserting supercookies into users' browser caches and into files associated with the latest version of the standard programming language used to build Web pages, known as HTML5.

In a blog post after the report was released, Kissmetrics said it would use only regular cookies for future tracking. The company didn't return calls seeking comment.

Write to Julia Angwin at julia.angwin@wsj.com