The Cookies You Can't Crumble

By Olga Kharif  August 21, 2014

If you’ve used the Internet for longer than the iPhone has been around, you’re probably familiar with cookies, those little packets of personal data that help load websites you frequent and tell the websites’ owners who you are and what you’re up to—information coveted by advertisers. Since Netscape programmer Lou Montulli invented the cookie 20 years ago, it’s become a cornerstone of the online display and search advertising business, valued at $35 billion a year in the U.S. Montulli says he designed the cookie to make the Web more efficient and calls its use as a tracking device an “unintended consequence.”

The good news for those who don’t like to be watched online is that cookies haven’t changed much in two decades, enough time to develop ways to stop them from gathering all that data. Browser security settings can limit or block cookies used by advertisers. Twelve percent of Firefox users around the world have opted into Mozilla’s do-not-track program, and Microsoft’s (MSFT) Internet Explorer and Apple’s (AAPL) Safari now block many cookies by default. Most mobile devices, including the iPhone, don’t allow use of cookies in apps.

The bad news for the privacy-conscious is that big Web companies and dozens of startups have begun testing or using cookie alternatives that are often more difficult to spot or disable. These programs “don’t have consumer controls already there,” says Montulli, a co-founder of Zetta, a cloud storage startup. “Once they go into effect, consumers have no ability to turn them off.”

Some programs track users by their IP addresses; others look at users’ operating systems and other factors. As of Aug. 1, anyone who wants to hawk new or updated Android apps in Google’s (GOOG) online store must catalog customers with Advertising ID, a unique number that corresponds to a particular customer. Google has confirmed that it’s working on ways to link mobile browser activity to app use. Advertising ID looks a lot like Apple’s system, Identifier for Advertising. In both cases, users can change their settings to limit tracking for advertising, but app makers keep finding ways around those restrictions. Facebook (FB), which can track user activity on any website that has a Like button, announced in June that it intends to ignore browsers’ do-not-track settings in order to better target ads. Its users can still opt out of some tracking by changing their browser settings at the website of the Digital Advertising Alliance, an industry group. Despite their new tracking methods, Apple, Google, and Facebook say they’re committed to making their data collection transparent and giving users control over their privacy settings.

Startups are promising advertisers that they can deliver, without cookies, data comparable to what the big Web companies collect. Earlier this year, AddThis in Vienna, Va., tested a technique called canvas fingerprinting, in which a website makes visiting computers draw an object and tells the machines apart based on slight variations. In May, more than 5 percent of the top 100,000 websites listed on Alexa Internet (AMZN), a traffic-ranking company, employed canvas fingerprinting to track visitors, according to researchers from Princeton University and the University of Leuven in Belgium who analyzed Alexa’s data. Whitehouse.gov, YouPorn, and dating service Plenty of Fish were among the sites the researchers
found monitoring users with canvas fingerprinting without a mention in their privacy policies. Whitehouse.gov and YouPorn didn’t respond to requests for comment; Plenty of Fish Chief Executive Officer Markus Frind says he uses canvas fingerprinting “to keep Internet scammers off the site.”

$35b

Annual value of U.S. online display and search advertising business

Startups such as BlueCava, Drawbridge, and Tapad sell tracking services and software that can link smartphones, tablets, PCs, and even Internet-connected televisions to a distinct though nameless person, to minimize the money spent targeting him with a campaign. The companies’ algorithms sift the details of each device’s Web use based on factors such as IP address, browsing patterns, and what the person is reading. When a PC searches for a car quote from the same location as a tablet checking auto financing or a smartphone mapping a route to a dealer, those data points are collected in one profile rather than three and sold to auto industry advertisers. BlueCava Executive Chairman Phil Myers says his software can identify users in a household with 90 percent accuracy within two weeks. “With mobile, people typically start in the 20 percent range,” he says. The four-year-old company’s service starts at $10,000 a month, and the company has doubled its clients to 16 in the past year, he says.

Megan Schickedanz, director of digital operations at Blue Chip Marketing Worldwide, an ad agency, says the use of techniques such as canvas fingerprinting is exploding partly because “advertisers feel they are less invasive.” Unlike cookies, they don’t require a tracker to be placed within a user’s browser.

“What this means is that people attempting to not be tracked will be tracked,” says Kurt Opsahl, deputy general counsel of the Electronic Frontier Foundation. So far, consumers’ main recourse against tracking has been software such as the EFF’s Privacy Badger, which can block canvas fingerprinting and has been downloaded 400,000 times since its release in May.

The new tracking tools lack consistent industry standards, and some ad agencies have hesitated to deploy them without opt-out mechanisms. “Although we can test these techniques, we won’t use them without this consensus,” says Brian Lesser, CEO of Xaxis, which sells ad targeting services. Industry groups including the Digital Advertising Alliance and Interactive Advertising Bureau say they’re developing guidance for tracking technology; industry group DigiTrust, formed in June, says it will propose a common standard by the end of the year.

Reaching industrywide consensus won’t be easy, says Jordan Mitchell, vice president of product at Rubicon Project (RUBI), an ad tech company and member of DigiTrust. “We are in an arms race right now,” he says. Demandbase, which targets businesses with ads by tracking IP addresses, claims it can triple the number of Fortune 1,000 companies visiting a customer’s website within 30 days. Clients include Adobe Systems (ADBE), American Express (AXP), Dell (DELL), Hewlett-Packard (HPQ), and Microsoft. CEO Chris Golec says Demandbase’s client list was up 40 percent this year, to 250, and its revenue almost doubled.

The bottom line: New tracking software and services are reshaping the market for search and display advertising online.

Kharif is a reporter for Bloomberg News and Bloomberg Businessweek in Portland, Ore.