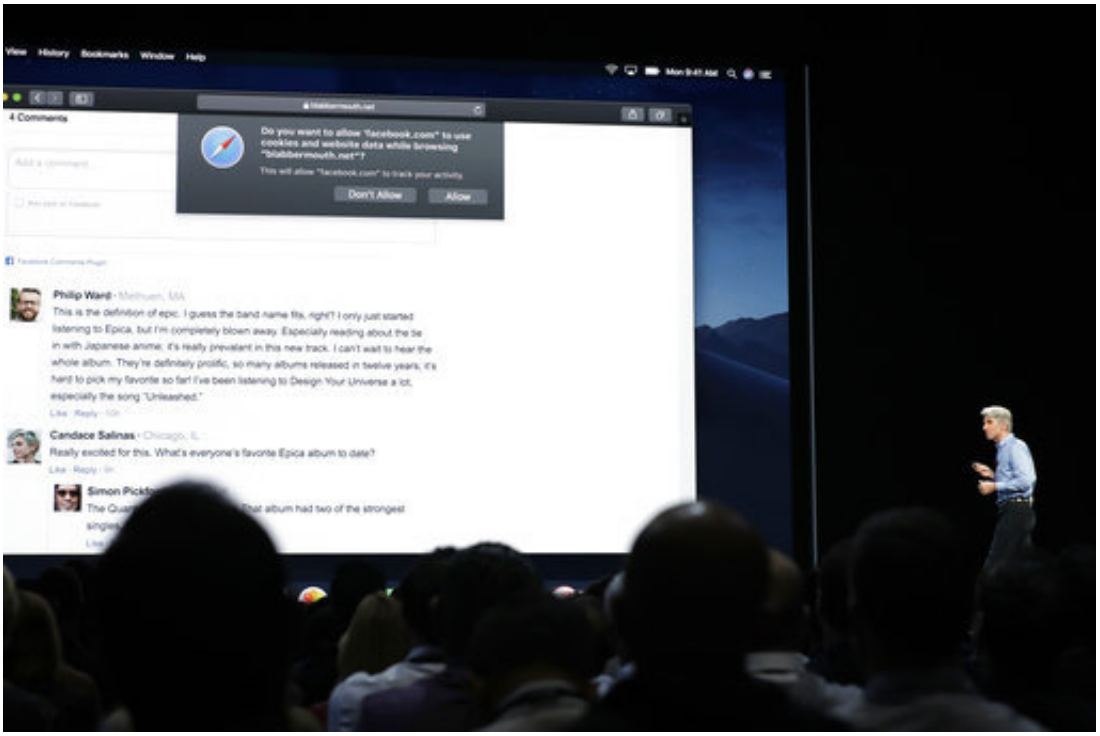
Apple, Firefox tools aim to thwart Facebook, Google tracking

September 14 2018, by Anick Jesdanun



In this June 4, 2018, photo Craig Federighi, Apple's senior vice president of Software Engineering, speaks during an announcement of new products at the Apple Worldwide Developers Conference in San Jose, Calif. Facebook and other companies routinely track your online surfing habits to better target ads at you. Two web browsers now want to help you fight back in what's becoming an escalating privacy arms race. New protections in Apple's Safari and Mozilla's Firefox browsers aim to prevent companies from turning "cookie" data files used to store sign-in details and preferences into broader trackers that take note of what you read, watch and research on other sites. (AP Photo/Marcio Jose Sanchez)

Facebook and other companies routinely track your online surfing habits to better target ads at you. Two web browsers now want to help you fight back in what's becoming an escalating privacy arms race.

New protections in Apple's Safari and Mozilla's Firefox browsers aim to prevent companies from turning "cookie" data files used to store sign-in details and preferences into broader trackers that take note of what you read, watch and research on other sites.

Lance Cottrell, creator of the privacy service Anonymizer, said Apple's effort was particularly significant, as it takes aim at a technique developed by tracking companies to override users' attempts to delete their cookies.

Safari makes these protections automatic in updates coming Tuesday to iPhones and iPads and a week later to Mac computers. Firefox has similar protections on Apple mobile devices and is rolling out them out to personal computers in the coming months.

To get the protections, you'll have to break your habit of using Google's Chrome browser, which by some estimates has more than half of the worldwide browser usage. Safari and Firefox have less than 20 percent combined.

Even then, Safari and Firefox can't entirely stop tracking. For starters, they won't block tracking when you're using Facebook or Google itself. Nor can they help much when you use phone or tablet apps, unless the app happens to embed Safari, as Twitter's iPhone app does.

But Will Strafach, a mobile security expert who is designing data security tools for phones, said imperfect protection is better than no protection. He notes that burglars can still break down a door, but that doesn't mean you shouldn't bother locking it.

Cookies and other trackers can be used by companies to keep track of who you are as you move from website to website. The companies can build a digital profile as you, say, read about Democratic or Republican viewpoints, buy a particular brand of pet food or indulge in the entire season of "Keeping Up With The Kardashians."

News, video and other third-party sites use Google and Facebook cookies to customize ads to your hobbies and interests, rather than hawking products you might never buy. That's why you might see an ad for shoes soon after searching for them elsewhere.

Apple says its tests show that some popular websites are embedded with more than 70 such trackers. Many of these are from Facebook and Google, which are expected to command a combined 57 percent of the $107 billion U.S. digital advertising market this year, according to the research group eMarketer.

Though general awareness of data collection has grown in the wake of Facebook's Cambridge Analytica privacy scandal , how trackers work behind the scenes remains a mystery to many people.

Ghostery and other products have long offered tracking protection. The browsers are now trying to incorporate that directly so you don't have to go looking for browser add-ons.

Safari will try to automatically distinguish cookies that are useful from ones that are there just to track you. Apple notes that cookies can appear in unexpected places, such as sites that embed "like" and "share" buttons. Now, those cookies will be blocked until you click on one of those buttons, in which case you'll be prompted for permission to allow the tracking. If you don't, your "like" won't register.

Safari is also attacking a technique developed to circumvent cookie

deletions. Through "fingerprinting," a company can identify you through your computer's characteristics, such as browser type and fonts installed. Your new cookie can then be tied to your old profile. Safari will now limit the technical details it sends.

Firefox has an anti-tracking feature that also tries to distinguish tracking cookies from useful ones. It's on by default only on Apple's mobile devices. Mozilla is testing a broader rollout for personal computers, though its plans for Android are not yet known. For now, you need to turn it on or use a private-browsing mode, which gets more aggressive at killing cookies, including useful ones.

For PCs, Firefox also has an optional add-on, called Facebook Container, to segregate your Facebook activity from everything else. Think of it as a wall that prevents Facebook from accessing its data cookie as you surf elsewhere. A version is available for other trackers, too, but requires configuration on your part.

None of the Firefox tools, though, address fingerprinting.

Unsurprisingly, advertisers aren't happy.

In a statement, Interactive Advertising Bureau executive Dennis Buchheim said that even as browsers makers feel pressured to deliver privacy-centric features, they should consider the importance of advertising in enabling free services.

The new Safari and Firefox tools don't block ads. But without cookies, websites might get paid a lot less for them, said Jed Williams, chief innovation officer at the Local Media Association, an industry group for news publishers.

Apple and Mozilla are able to push the boundaries on privacy because

neither depends on advertising. Google makes most of its money from selling ads.

Facebook and Google declined comment on the Safari and Firefox tools. But Google said its Chrome browser offers tools to control and delete cookies and set preferences for certain websites. Google says users can also decline personalization and get generic ads instead, though tracking continues in the background while using the company's services.

How Apple's Safari browser will try to thwart data tracking

New privacy features in Apple's Safari browser seek to make it tougher for companies such as Facebook to track you.

Companies have long used cookies to remember your past visits. This can be helpful for saving sign-in details and preferences. But now they're also being used to profile you in order to fine-tune advertising to your tastes and interests.

Cookie use goes beyond visiting a particular website. As other sites embed Facebook "like" and "share" buttons, for instance, Facebook's servers are being pinged and can access your stored cookies. That means Facebook now knows you frequent celebrity gossip sites or read news with a certain political bent. Ads can be tailored to that.

Here's how Safari is getting tougher in dealing with that.

NO MORE GRACE PERIOD

Safari used to wait 24 hours from your last visit to a service before blocking that service's cookies on third-party sites. That effectively

exempted Facebook, Google and other services that people visited daily. Now, Safari will either block the cookie automatically or prompt you for permission.

Apple says Safari will still be able to remember sign-in details and other preferences, though some websites have had to adjust their coding.

THWARTING FINGERPRINTING

Browsers typically reveal seemingly innocuous information about your device, such as the operating system used and fonts installed. Websites use this to make minor adjustments in formatting so that pages display properly.

Browsers have historically made a lot of information available, largely because it seemed harmless. Now it's clear that all this data, taken together, can be used to uniquely identify you. Safari will now hide many of those specifics so that you will look no different from the rest.

It's like a system that digitally blurs someone's image, said Lance Cottrell, creator of the privacy service Anonymizer. "You can tell it's a person and not a dog, but you can't recognize a person's face," he said.

For instance, Safari will reveal only the fonts that ship with the machine, not any custom fonts installed.

MASKING WEB ADDRESSES

When visiting a website, the browser usually sends the web address for the page you were just on. This address can be quite detailed and reveal the specific product you were exploring at an e-commerce site, for instance.

Now, Safari will just pass on the main domain name for that site. So it would be just "Amazon.com" rather than the specific product page at Amazon.

CLOSING A LOOPHOLE

Some ad companies have sought to bypass restrictions on third-party cookies—that is, identifiers left by advertisers—by using a trick that routed them through a series of websites. That could make a third-party cookie look like it belonged to a site you're visiting. Safari will now try to catch that.

The changes come Tuesday as part of the iOS 12 update for iPhones and iPads and a week later in the Mojave update for Mac computers.

Many of the safeguards will be limited to cookies that Apple deems to be trackers. That's being done to reduce the likelihood of inadvertently blocking legitimate third-party cookies.