

EX1049

HOME · COMPUTING · FEATURES

Are cookies crumbling our privacy? We asked an expert to find out

By Simon Hill March 29, 2015



Image used with permission by copyright holder

"Cookies are just a fundamental part of how the Web works, about as essential as Wi-Fi, HTML, or electricity," explains [Silktide](#) founder, Oliver Emberton. "All cookies do is recognize your computer as it travels between Web pages — so you need them for critical things like logging into a website, or buying something from a store."

Cookies are small text files that reside on your computer, and the information they contain is set and accessed by the servers of the websites that you visit. Cookies allow servers to identify you and remember things about you.

Recommended Videos

"The problem is that those same cookies can also be used to track people, and do things that many people don't like, like deliver targeted ads," says Emberton. "And this has got a lot of people understandably concerned."

Related

- [Is ChatGPT creating a cybersecurity nightmare? We asked the experts](#)
- [Do mental health apps really help? We asked the experts](#)
- [How is 5G helping businesses in the U.S. right now? We asked the experts](#)

In Europe, it generated so much concern that the European Union legislated in 2011, demanding that websites gain user consent to use cookies. That law is still the subject of much debate, but before we get into it, let's rewind and take a look at where cookies came from in the first place.

A brief history of cookies

The man responsible for cookies is [Lou Montulli](#). He developed one of the earliest Web browsers, Lynx, in 1991 and joined Mosaic Communications Corporation, later to become Netscape, in 1994. He was responsible for a variety of Web innovations including the blink tag, server push and client pull, HTTP proxying, and cookies.

According to the man himself, cookies are named after the computer science term "magic cookie," as discovered by [Clouseau on Google Answers](#). The [Jargon File](#) describes a magic cookie as "something passed between routines or programs that enables the receiver to perform some operation; a capability ticket or opaque identifier."

"The vulnerability of systems to damage or snoop by using Web browser cookies is essentially nonexistent."

Montulli had the idea to use a similar system in the Netscape browser for Web communications, and he used the familiar programming term, cookie. They were first used to verify whether users had visited the Netscape website before, and they enabled websites to remember your preferences. The cookies also presented a handy solution for virtual shopping carts, enabling e-commerce websites to remember what you were shopping for the last time you visited.

The public didn't really become aware of them until 1996, when the media started reporting on the potential threat to privacy. Concerns focused on the fact that cookies were storing information on user's computers without their knowledge or consent.

The revelation generated enough fuss that in 1998, the U.S. Department of Energy Computer Incident Advisory Capability released an [information bulletin](#), which included this assessment: "The vulnerability of systems to damage or snooping by using Web browser cookies is essentially nonexistent. Cookies can only tell a Web server if you have been there before and can pass short bits of information (such as a user number) from the Web server back to itself the next time you visit. ...

Information about where you come from and what Web pages you visit already exists in a Web server's log files and could also be used to track users browsing habits, cookies just make it easier."

What is the threat?

Clearly cookies have an important function, and they make Web browsing much more convenient for us, since we don't have to identify ourselves again every time we visit a website. Many people don't see much of an issue with cookies, but the potential threat is described succinctly on [Cookie Central](#):

"Unfortunately, the original intent of the cookie has been subverted by some unscrupulous entities who have found a way to use this process to actually track your movements across the Web. They do this by surreptitiously planting their cookies and then retrieving them in such a way that allows them to build detailed profiles of your interests, spending habits, and lifestyle.

On the surface, this practice may seem harmless and hardly worth fretting over since the worst thing most imagine is that corporate concerns will use this information to devise annoying, yet relatively innocuous advertising campaigns, targeted towards specific groups or individuals. However, it is rather scary to contemplate how such an intimate knowledge of our personal preferences and private activities might eventually be used to brand each of us as members of a particular group.

But remember a site only knows what information you have entered. Not all cookies are bad, they can also provide useful functions on the Web. The threat posed by cookies is a legitimate concern for people worried about privacy, but it pales in comparison to other threats, particularly in the wake of [Edward Snowden's revelations](#) about the NSA and government surveillance.

Cookies are the thin end of the wedge

"Cookies aren't the problem," says Emberton. "There are equivalent or worse technologies that most people don't know about (like local storage and LSOs), which can do the same thing. Cookies just happen to have caught mainstream awareness. The real issue isn't the technology, it's what people choose to do with it, but that's harder to police."

"Over 95 percent of websites use cookies, mostly for boring things that never cross our minds, like ensuring a website responds quickly, or counting visitors. The data most sites hold can't be used to identify you personally," he explains. "However, a handful of big companies — most notably Google, [Facebook](#), and Amazon — hold a vast amount of personally identifiable information about millions of people. For example, Google's history might tell someone if you have a medical problem, or your sexual orientation, or what political party you support. This information is likely linked to your real name."

"Google's history might tell someone if you have a medical problem, your sexual orientation, or what political party you support."

The FTC has tangled with Google and others on the issue of online privacy several times in the last few years. In 2012 [Google agreed to a \\$22.5 million settlement](#) over Apple's Safari Web browser, which has a default setting to block third-party cookies that Google bypassed. A U.K. court recently ruled that [Safari users can sue](#) Google over cookie tracking.

In the States, there have been attempts to introduce "Do Not Track" legislation, mirroring the "Do Not Call" law, which prevents telemarketers from contacting people who opt out. The idea is to give users the right to opt out of being tracked by third-party websites. According to its website, as part of its remit to protect consumer privacy, the FTC has been considering the "Do Not Track" proposal, but has yet to vote on whether to support it.

From 2011 various bills have been introduced, but later withdrawn or failed. The difficulty of establishing standards and agreeing workable legislation seems to have scuppered its progress. By contrast, legislation was passed in the EU, but how effective it has been in protecting consumer privacy is highly questionable.

EU Cookie law

In May, 2011, the e-Privacy Directive changed the law with regard to cookies in the European Union. In order to comply with the new law, website owners were charged with telling visitors about the cookies they use and obtaining their consent. In practice, websites that have complied now display a pop-up when you first visit that links to an explanation of their cookie policy and allows you to accept it.

European website owners and online businesses were understandably upset. Particularly because the law could penalize them, but not their competitors beyond EU jurisdiction. At first it wasn't clear how the legislation would be enforced.

In the U.K., it fell to the Information Commissioner's Office (ICO) to decide, and the agency gave websites a grace period of a year to comply. Many did comply, in no small part because the ICO was empowered to impose fines of up to £500,000 (\$768,000), but the lack of will to enforce the law across the EU soon led to resistance.

Silktide develops software to help measure website quality. It released a free, open source cookie consent plug-in to enable websites to easily comply with the new law, but then it decided to challenge the ICO with nocookielaw.com, which begins "Dear ICO, Sue us," and goes on to ridicule the law and explain why it's largely pointless.

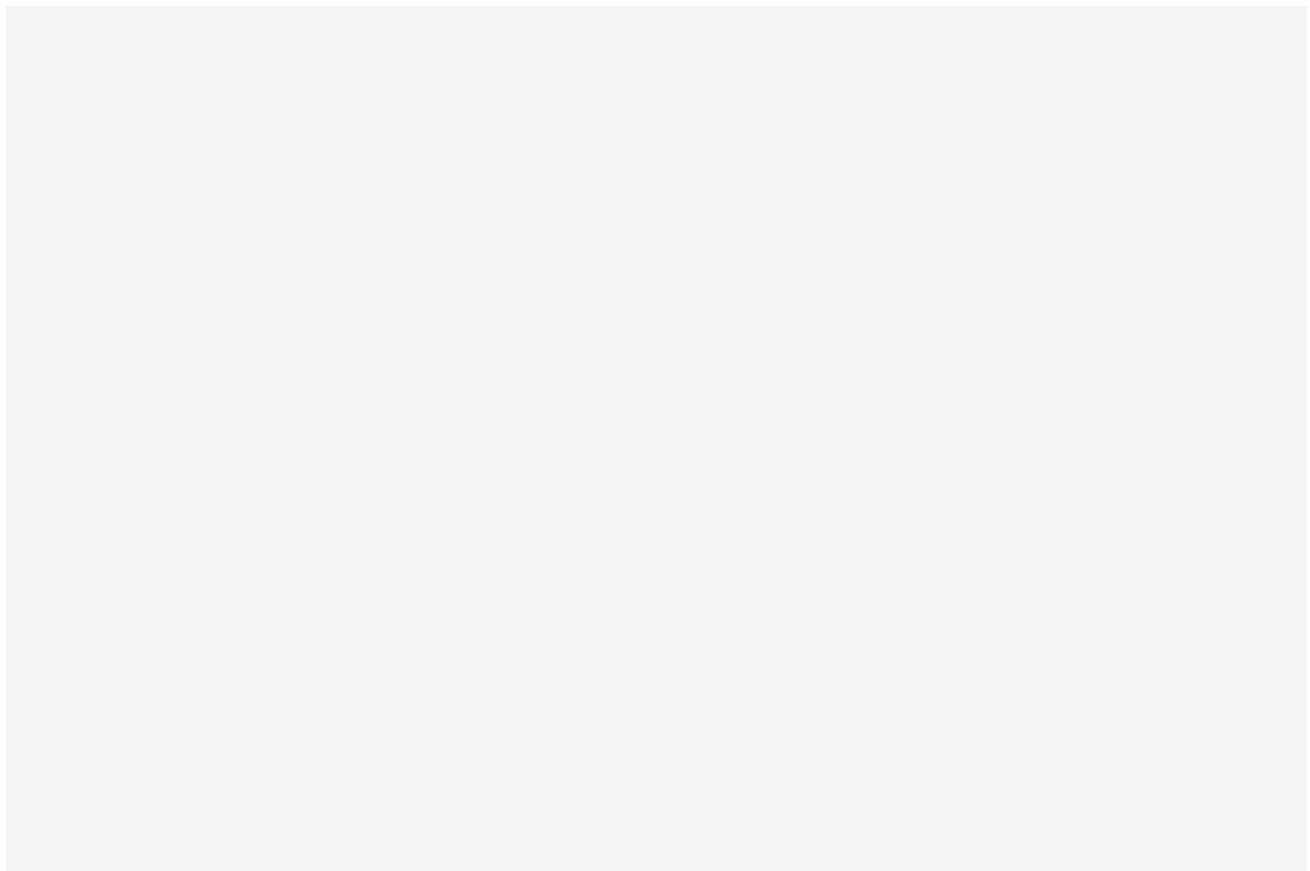


Image used with permission by copyright holder

There was no lawsuit. We contacted the ICO, and Lead Communications Officer Anya Burgess confirmed that "so far the ICO have not issued any fines for ignoring the EU cookie law."

She also pointed us to ICO's latest study, which reveals the average website places 34 cookies on your device on your first visit, and 70 percent of them were third-party cookies (set by websites other than the one being visited). The study also

raises concerns about the expiry dates on cookies, with some, optimistically, set to expire in the year 9999.

"I find the law misguided, but it has softened over the last couple of years, as the EU wrestled with how to implement it," says Silktide's Emberton. "The difference between what was written — which pretty much made every website illegal — and what has been policed is immense. I expect the letter of the law will slowly catch up with reality over time, but I don't expect the law will actually do anything for user's privacy."

That's the way the cookie crumbles

There are still efforts in motion to get some legislation on the books Stateside, but resistance remains fierce, and even if some kind of "Do Not Track" law is passed, will the FTC have the power or the will to enforce it against big business?

"Improving online privacy would be a noble goal, but regulating cookies would be a terrible way to accomplish it," says Emberton when asked about the U.S.

"Cookies by themselves pose no threat to the average person, but the information that companies store about you (with or without cookies) is always a concern, and should be protected for good reason."

Editors' Recommendations

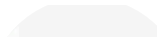
- [Does your Mac need antivirus software in 2024? We asked the experts](#)
- [We asked the experts if biological sex affects heart rate sensor accuracy](#)
- [DuckDuckGo calls out Google privacy update for 'creepy advertising'](#)
- [Is jelly scrolling on the iPad Mini really normal behavior? We asked the experts](#)
- [Is Mac really more secure than Windows? We asked the experts](#)

Topics

[Mobile](#)

[Web](#)

[Features](#)



Simon Hill

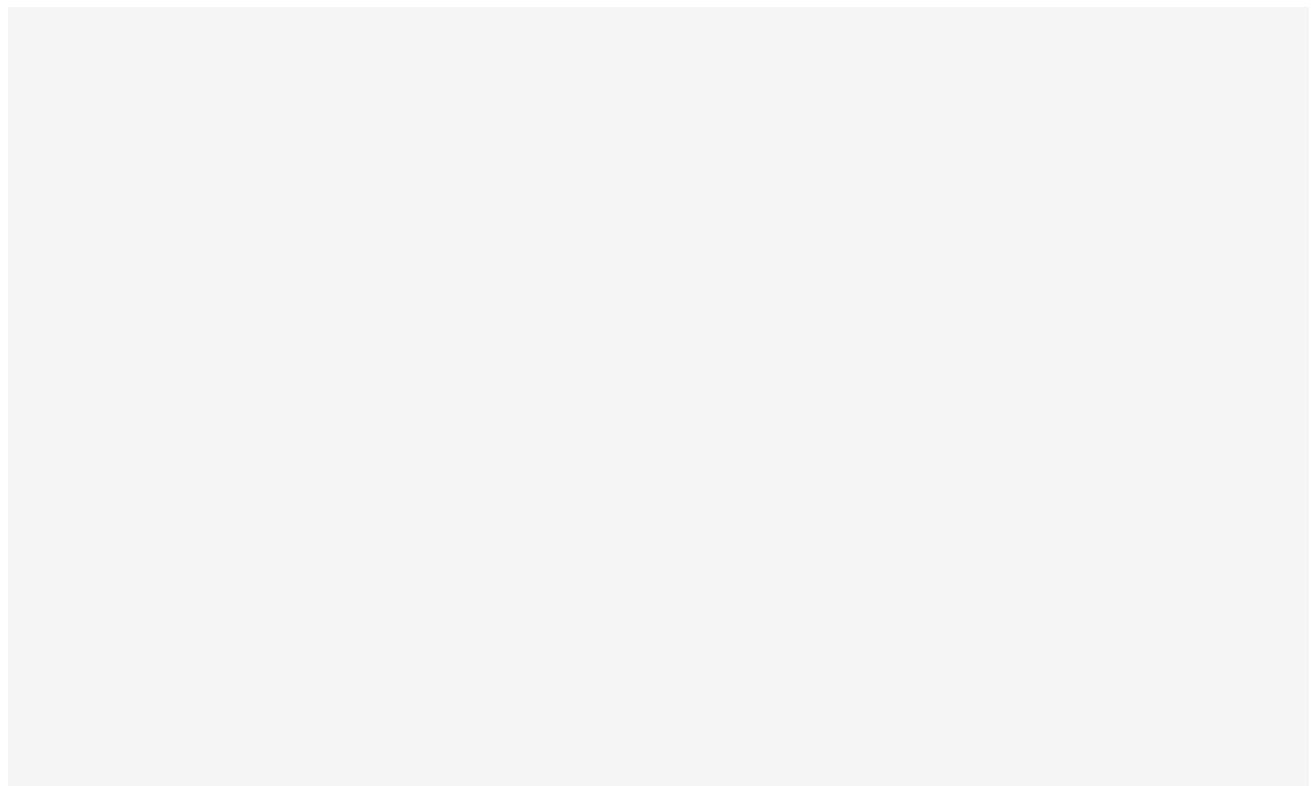
Former Digital Trends Contributor



Simon Hill is an experienced technology journalist and editor who loves all things tech. He is currently the Associate Mobile...

COMPUTING

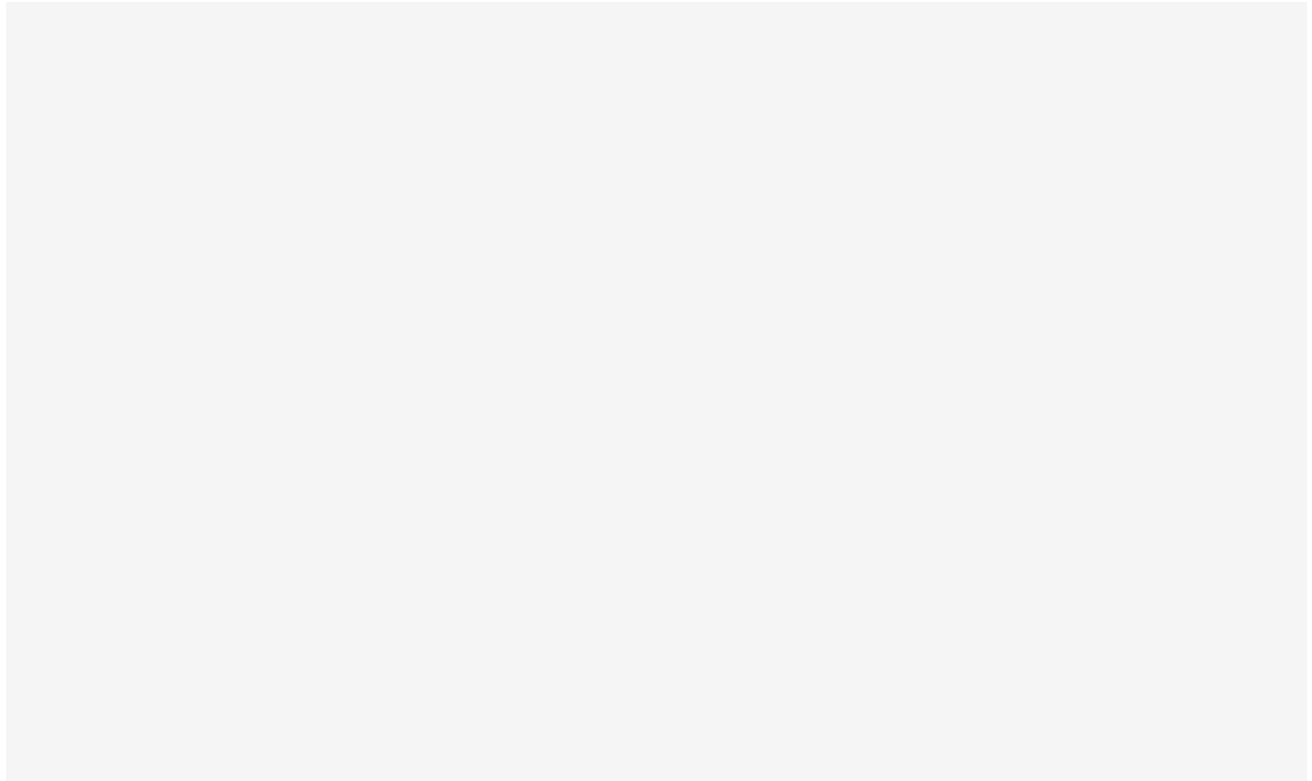
Apple says Mac Catalyst is working. We asked developers to find out the truth



Apple's Mac Catalyst project seems harmless enough. It provides a simple way for iOS developers to bring their apps to the Mac -- a win-win scenario for both developers and Apple, right? Well, yes. But if you're judging by history, the stakes are high. Bridging the gap between the worlds of mobile and desktop appears a...

[Read more](#)

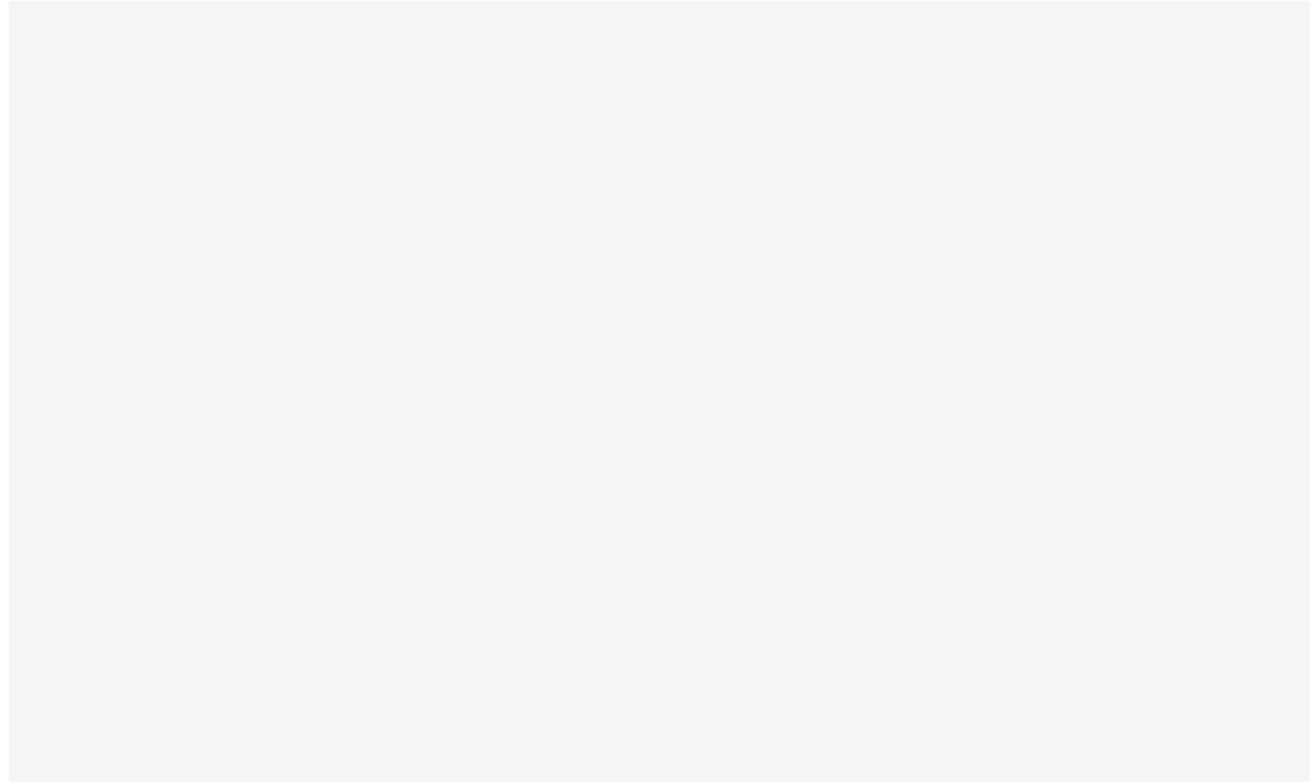
Does tracking your sleep actually help you sleep better? We asked an expert



Modern life simply isn't conducive to getting a good night's sleep. There's artificial light everywhere, we spend hours glued to screens, and it's not unusual to be checking work emails on your phone at night, last thing before you go to bed. We know that the potential health consequences of not getting enough sleep are seve...

[Read more](#)

The wait for a cheaper Vision Pro is going to be a long one



It looks like a more affordable take on the \$3,500 Vision Pro mixed-reality headset has taken a backseat at Apple. In January this year, The Information reported that a lower-priced version with toned-down innards could arrive in 2025. Now, renowned supply chain analyst Ming-Chi Kuo claims that the pocket-friendly headset won't b...

[Read more](#)

Upgrade your lifestyle

Digital Trends helps readers keep tabs on the fast-paced world of tech with all the latest news, fun product reviews, insightful editorials, and one-of-a-kind sneak peeks.



Mobile

Computing

Gaming

Audio / Video

Smart Home

Entertainment

Automotive

Space

Streaming Guides

Original Shows

Downloads

How-To

About Us

Contact Us

Editorial Guidelines

Logo & Accolade Licensing

Subscribe to our Newsletter

Branded Content

Digital Trends Wallpapers

Digital Trends in Spanish

Portland | New York | Chicago | Detroit | Los Angeles | Toronto

[Careers](#)

[Privacy Policy](#)

[Advertise With Us](#)

[Do Not Sell or Share My Information](#)

[Work With Us](#)

[Manage Preferences](#)

[Diversity & Inclusion](#)

[Press Room](#)

[Terms of Use](#)

[Sitemap](#)

Digital Trends Media Group may earn a commission when you buy through links on our sites.

