**What is Evercookie and how does it work?**

To recap, both of the regulations discussed above allow for the use of cookies, but the user must have the choice to opt out or remove cookies at any time. Seems fair and logical. But in reality things aren’t so rosy. There are shady mechanisms for tracking.

To be precise, there are tools that circumvent the user’s privacy choices and install permanent cookies that can be recovered after deletion.

But how is that possible? This is what Evercookie does. Don’t get misled by the name, it’s not an actual cookie. It’s a JavaScript programming library that produces cookies allowing you to identify users even after they’ve deleted their standard cookies, Flash cookies (Local Shared Objects or LSOs), and other ones. Even when a user erases cookies, those files are recreated and continue to perform their task.

According to the creator of Evercookie, programmer Samy Kamkar, Evercookie is designed to make **persistent data** just that – persistent. The process isn’t complicated. He explains that since the same data is stored in different browser storage locations, if any of the data is lost it can simply be recovered and stored for re-use.

Evercookie is producing those super cookies – persistent cookies – you’ve probably heard about. They rely on tricky techniques and are really hard to delete.

The API we’ve mentioned just stores cookie data in different places in the local browser. If Evercookie learns that the user has removed some cookies hiding in a dark corner of the browser, it creates them again. It uses JavaScript to **re-spawn cookies**. And it does so without the user’s knowledge, never mind consent.

To be precise, when Evercookie creates a new cookie, it applies **storage mechanisms** such as:

* standard HTTP Cookies
* HTTP Strict Transport Security (HSTS) Pinning
* Local Shared Objects (Flash Cookies)
* Silverlight Isolated Storage
* storing cookies in Web History
* storing cookies in HTTP ETags
* storing cookies in Web cache
* Internet Explorer userData storage
* HTML5 Session, Local and Global Storage
* HTML5 Database Storage via SQLite
* Java JNLP PersistenceService

Kamkar developed Evercookie to spread awareness of privacy risks and bring to light how easily companies can track users while disrespecting their preferences.

**Customer Data Platform vs. Data Management Platform**

Learn over 25 key differences between Customer Data and Data Management platforms and decide which of them will be a better fit for your business

[Download FREE Comparison](https://campaign.piwik.pro/dmp-vs-cdp/)

**Evercookie and compromises to user privacy**

It’s no surprise that the process of **re-spawning cookies** has been widely condemned. It definitely **violates users privacy rights**. It tramples on users’ explicit wishes. When a user erases a cookie, this is a deliberate action that needs to be respected.

What’s more, Evercookie can exploit user’s browser history or hidden properties of browser windows (the window’s label, invisible to the user, which is transmitted during every transaction).

Furthermore, dealing with persistent cookies is a futile undertaking. Routinely deleting caches can be helpful, but users may not be able to remove all elements. Using private mode browsing can be a good solution in certain circumstances. However, it’s not always convenient as you often need to rely on persistent logins. And one last tip: keep your browser up-to-date.

Users are becoming increasingly aware of and concerned with shady tracking practices. One way they take care of online privacy is by adjusting browser settings.

The trouble is that each browser can have different settings, and not all of them offer a clear settings allowing users to remove all data stored by trackers. This means that deleting data like permanent cookies is getting tougher and tougher, involving a lot more steps.

What’s more, the increasing number of ways to store this data is making it even harder for browser manufacturers to keep up and provide better pro-privacy solutions.