**Evercookie** (also known as supercookie[[1]](https://en.wikipedia.org/wiki/Evercookie" \l "cite_note-:0-1)) is a JavaScipt [API](https://en.wikipedia.org/wiki/API) that identifies and reproduces intentionally deleted cookies on the clients' browser storage.[[2]](https://en.wikipedia.org/wiki/Evercookie#cite_note-2) Websites that have adopted this mechanism can identify users even if they attempt to delete the previously stored cookies.[[3]](https://en.wikipedia.org/wiki/Evercookie#cite_note-:2-3) It was created by [Samy Kamkar](https://en.wikipedia.org/wiki/Samy_Kamkar" \o "Samy Kamkar) in 2010 to demonstrate the possible infiltration from the websites that use respawning. [[4]](https://en.wikipedia.org/wiki/Evercookie#cite_note-4)

In 2013, [Edward Snowden](https://en.wikipedia.org/wiki/Edward_Snowden) leaked a top-secret [NSA](https://en.wikipedia.org/wiki/National_Security_Agency) document that showed Evercookie can track [Tor](https://en.wikipedia.org/wiki/Tor_(anonymity_network)) (anonymity networks) users.[[5]](https://en.wikipedia.org/wiki/Evercookie#cite_note-:1-5) Many popular companies use functionality similar to Evercookie to collect user information and track users. [[1]](https://en.wikipedia.org/wiki/Evercookie#cite_note-:0-1) Further research on fingerprinting and search engines also draws inspiration from Evercookie's ability to persistently track a user. [[3]](https://en.wikipedia.org/wiki/Evercookie#cite_note-:2-3)[[5]](https://en.wikipedia.org/wiki/Evercookie#cite_note-:1-5)

Background[[edit](https://en.wikipedia.org/w/index.php?title=Evercookie&action=edit&section=1)]

A traditional [HTTP cookie](https://en.wikipedia.org/wiki/HTTP_cookie) is a relatively small amount of textual data that is stored by the user's browser. Cookies can be used to save preferences and login session information; however, they can also be employed to track users for marketing purposes. Due to concerns over privacy, all major browsers include mechanisms for deleting and/or refusing to accept cookies from websites.

[Adobe Systems](https://en.wikipedia.org/wiki/Adobe_Systems) claimed that the size restrictions, likelihood of eventual deletion, and simple textual nature of traditional cookies motivated it to add the [local shared object](https://en.wikipedia.org/wiki/Local_shared_object) (LSO) mechanism to the [Adobe Flash Player](https://en.wikipedia.org/wiki/Adobe_Flash_Player).[[6]](https://en.wikipedia.org/wiki/Evercookie#cite_note-6) While Adobe has published a mechanism for deleting LSO cookies (which can store 100 KB of data per website, by default),[[7]](https://en.wikipedia.org/wiki/Evercookie#cite_note-7) it has met with some criticism from security and privacy experts.[[8]](https://en.wikipedia.org/wiki/Evercookie#cite_note-8) Since [version 4](https://en.wikipedia.org/wiki/Firefox_4), Firefox has treated LSO cookies the same way as traditional HTTP cookies, so they can be deleted together.[[9]](https://en.wikipedia.org/wiki/Evercookie#cite_note-firefox_flash_LSO_semantic_change_implementation1-9)[[10]](https://en.wikipedia.org/wiki/Evercookie#cite_note-firefox_flash_LSO_semantic_change_implementation2-10)

## Description[[edit](https://en.wikipedia.org/w/index.php?title=Evercookie&action=edit&section=2)]

[Samy Kamkar](https://en.wikipedia.org/wiki/Samy_Kamkar) released v0.4 beta of the Evercookie on September 13, 2010, as [open source](https://en.wikipedia.org/wiki/Open-source_license).[[11]](https://en.wikipedia.org/wiki/Evercookie#cite_note-auto-11)[[12]](https://en.wikipedia.org/wiki/Evercookie#cite_note-12)[[13]](https://en.wikipedia.org/wiki/Evercookie#cite_note-13) According to the project's website:

Evercookie is designed to make persistent data just that, persistent. By storing the same data in several locations that a client can access, if any of the data is ever lost (for example, by clearing cookies), the data can be recovered and then reset and reused.

Simply think of it as cookies that just won't go away.

Evercookie is a javascript API available that produces extremely persistent cookies in a browser. Its goal is to identify a client even after they've removed standard cookies, Flash cookies (Local Shared Objects or LSOs), and others.

Evercookie accomplishes this by storing the cookie data in several types of storage mechanisms that are available on the local browser. Additionally, if Evercookie has found the user has removed any of the types of cookies in question, it recreates them using each mechanism available.

An Evercookie is not merely difficult to delete ⁠— ⁠it actively "resists" deletion by copying itself in different forms on the user's machine and resurrecting itself if it notices that some of the copies are missing or expired.[[14]](https://en.wikipedia.org/wiki/Evercookie#cite_note-14) Specifically, when creating a new cookie, Evercookie uses the following storage mechanisms when available:

* Standard HTTP cookies
* local shared objects (Flash cookies)
* [Silverlight](https://en.wikipedia.org/wiki/Microsoft_Silverlight) Isolated Storage
* Storing cookies in RGB values of auto-generated, force-cached [PNGs](https://en.wikipedia.org/wiki/Portable_Network_Graphics) using [HTML5 Canvas tag](https://en.wikipedia.org/wiki/Canvas_element) to read pixels (cookies) back out
* Storing cookies in [Web history](https://en.wikipedia.org/wiki/Web_browsing_history)
* Storing cookies in [HTTP ETags](https://en.wikipedia.org/wiki/HTTP_ETag)
* Storing cookies in [Web cache](https://en.wikipedia.org/wiki/Web_cache)
* window.name caching
* [Internet Explorer](https://en.wikipedia.org/wiki/Internet_Explorer) userData storage
* HTML5 Session [Web storage](https://en.wikipedia.org/wiki/Web_storage)
* HTML5 Local [Web storage](https://en.wikipedia.org/wiki/Web_storage)
* HTML5 Global Storage
* HTML5 [Web SQL Database](https://en.wikipedia.org/wiki/Web_SQL_Database) via [SQLite](https://en.wikipedia.org/wiki/SQLite)

The developer is looking to add the following features, among others:[[15]](https://en.wikipedia.org/wiki/Evercookie#cite_note-15)

* Caching in [HTTP Authentication](https://en.wikipedia.org/wiki/Basic_access_authentication)
* Using [Java](https://en.wikipedia.org/wiki/Java_(programming_language)) to produce a unique key based on [NIC](https://en.wikipedia.org/wiki/Network_interface_controller) information.

## See also[[edit](https://en.wikipedia.org/w/index.php?title=Evercookie&action=edit&section=3)]

* [Device fingerprint](https://en.wikipedia.org/wiki/Device_fingerprint)
* [Canvas fingerprinting](https://en.wikipedia.org/wiki/Canvas_fingerprinting)
* [HTTP cookie](https://en.wikipedia.org/wiki/HTTP_cookie)
* [Flash cookie (Local shared object)](https://en.wikipedia.org/wiki/Local_shared_object)
* [Web storage](https://en.wikipedia.org/wiki/Web_storage)
* [Indexed Database API](https://en.wikipedia.org/wiki/Indexed_Database_API)
* [Web SQL Database](https://en.wikipedia.org/wiki/Web_SQL_Database)
* [Google Gears](https://en.wikipedia.org/wiki/Google_Gears)