Cookies You Can't Eat

Paul S. Wang, Sofpower.com

February 5, 2025

We all love cookies, sweet and tasty! But here, we are talking about a different kind of cookie–the cookies used by websites and browsers (Figure 1). Such cookies are **stored data** to make your web surfing easier, more effective and efficient. Cookies are basically unavoidable for anyone who goes online. Therefore, we all need to face dealing with them head-on.

We'll look at web cookies, what they are, why they are needed, and what pitfalls they may bring. With such understanding, we can better deal with cookies and manage permissions to their use in different situations.

Figure 1: Web Cookies

This article is part of our *Computational Thinking* (CT) blog. You can find other interesting articles in *aroundKent* (`aroundkent.net`), an online magazine. You can also find many such articles in the author's book *Becoming A Computational Thinker: Success in the Digital Age*. See the website `computize.org/CTer` for more information.

Let's begin by looking at the web, how it works and why it needs cookies.

How the Web Works

The web is formed by many *web servers* on the Internet. They offer various services online, including news, shopping, banking, entertainment, learning, healthcare, social media, and many more. Indeed, modern living depends on the web.

We, the users, use a client app to obtain the contents provided by the servers. A client app is usually a web browser such as Google Chrome, Firefox, MS Edge, and Apple Safari. Of course, this follows the typical Internet client-and-server communication model (Figure 2).

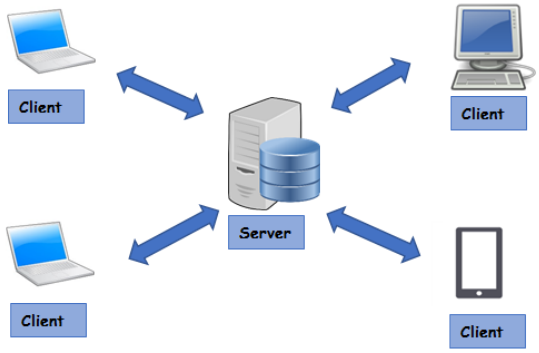

Figure 2: Client And Server Model

A web client communicates with any web server through a specific protocol, namely the Hypertext Transfer Protocol (HTTP)[1]. Here is a way to visualize client-server interactions via HTTP:

1. A client sends a **request**: A browser sends an *HTTP request* to the server. The request indicates the specific information to get (download) from the server and, sometimes, also supplies data to the server. In the simplest case, a request can just ask for a webpage.

2. The server sends a **response**: The receiving web server will process the request and send back an *HTTP response* to the browser. And the interaction is **complete**.

[1]Many modern websites use **HTTPS** which is HTTP with secure data transport.

In other words, an HTTP request is like a letter sent to the server and the HTTP response is like a reply letter. After the response, the server is **not required to remember the request or response** and usually forgets it entirely. Thus, for HTTP, every request-response pair is self-contained and independent of any other. This property is described as the **stateless** nature of the HTTP protocol.

Implications of Statelessness

The HTTP being stateless makes it easy for web servers to become efficient, scalable and robust, among other advantages. HTTP remains stateless to this day.

However, the statelessness does present a serious shortcoming, namely **a way is needed to connect related client requests**. When calling customer service, do you get annoyed when the other end keeps asking you to repeat the same information after being transferred? To further illustrate this, let's visualize an imagined stateless pizza store.

Figure 3: Movie Momento

You, the client, call the pizza store and order a hand-tossed pizza. The pizza place replies with an "order received" message, and ends the call. So far so good. Now, you want to add some pepperoni topping. So, you call

again sending another request. **But the stateless store has no way to know which pizza order needs the topping!** Now that would be very frustrating indeed.

Sure, you can order the pizza with the topping in the first place. But what if later you wish to cancel the order or change the pick-up time? The fact is, some business requires more than one request-response step between the client and the server.

Like in the famous movie *Memento* (Figure 3), websites all have serious *memory loss* problem and a way must be found to fix that. **The remedy is cookies**!

What Are Website Cookies

A **cookie** is a piece of data that a web server asks a client (browser) to store (save) in the memory on your computing device. A copy of the cookie (data) is automatically sent back to the same server with every future request. Imagine that the stateless pizza store can tell you, the client, to remember *an order number* for example. You would present this order number (cookie) in any future request. Obviously, this solves the problem we discussed earlier.

A web server uses the HTTP `Set-Cookie` header in its response to save cookie data on the client side. Cookie data are usually in the form of one or more *attribute*=*value* pairs, `order=123456` for example.

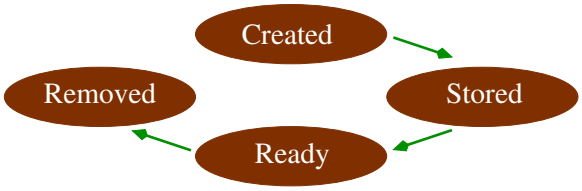

Figure 4: Cookie Lifecycle

A cookie undergoes the following lifecycle: *created by the website*, *stored in the browser*, *ready to be automatically sent to the same server upon later visits via the* `Cookie` *HTTP header*, *removed or expired at the end* (Figure 4).

The cookie was invented by Lou Montulli, a programmer at Netscape Communications, in 1994[2]. And the use of cookies basically solved the prob-

[2]The Netscape Navigator is the predecessor to Firefox

lem of remembering user-specific data for subsequent requests (webpage visits).

Cookie Examples

Thus, a website can use cookies to connect earlier steps to later ones for users in multi-step procedures as well as certain other situations.

Here's a list of common cookie uses, explained in simple terms with clear examples to help everyone see how cookies make the web more functional and convenient.

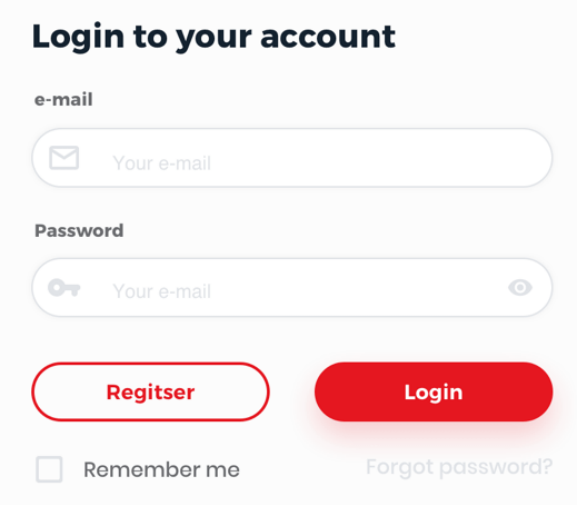

Figure 5: A Typical Login Screen

1. **Session Control**: A session is a sequence of related steps. Cookies help websites remember you while you're browsing so you don't have to log in or start over on every page. For example, when you log into your email, a session is created using cookies (Figure 5). Thus, when you move between your inbox, drafts, and sent folders the email site knows it is you. Such login sessions are widely used.

2. **Shopping Carts**: Cookies keep track of the items you add to your cart while shopping online. You're browsing amazon.com and add a pair of shoes to your cart. Even if you click away to look at other items, the shoes stay in your cart, thanks to cookies.

3. **User Preferences**: Cookies remember your settings, like language, display theme (dark mode), or font size, so you don't have to reconfigure them every time you visit. For example, a news website displays articles in your preferred language or display mode because cookies saved those settings.

4. **Video Resumption**: Cookies save where you stopped watching a video, so you can pick up where you left off later. For example, on YouTube, you pause a video at time stamp 3:15, say. When you return later, the video starts playing from 3:15.

5. **Login Status**: Cookies help websites remember that you have logged in before using the same computer and browser. For example, you go to a site such as amazon.com or temu.com and the website recognizes you and signs you in automatically.

6. **Personalized Recommendations**: Cookies track what you've looked at or searched for to suggest similar products or content. For example, you browse sneakers on an online store. Later, the site suggests matching socks or more sneakers based on your earlier browsing.

7. **Analytics and Performance**: Cookies help website owners understand how visitors use their site, like which pages are popular or where users drop off. For example, a business sees that most people leave their website after visiting the pricing page. They use this insight to improve the page or even the prices.

8. **Targeted Advertising**: Cookies track your browsing habits across sites to show you ads that match your interests. For example, you search for vacation packages on one website, and later you see ads for flights and hotels on other unrelated websites.

9. **Fraud Prevention and Security**: Cookies help websites detect suspicious activity, like multiple failed login attempts or fraudulent transactions. For example, your bank uses cookies to recognize your usual device. If someone tries to log in from a new device, the bank might ask for extra verification.

These examples illustrate the broad range of ways cookies enhance our online experiences in everyday life. And we see how cookies make the web

more convenient by remembering our actions, preferences, and data. While they're incredibly useful, understanding their purpose helps users make better choices about accepting or rejecting cookies.

Cookies And Privacy Concerns

Cookies are used by websites in many ways, including shopping carts, authentication (login session), personal preferences (remembering themes/layouts), *analytics* (tracking user behavior across a site or multiple visits), advertising (targeting ads based on browsing behavior).

Functional cookies are critical for the website to work and they typically do not require *user consent* as they provide critical functionality. Other cookies, such as analytics cookies, advertising cookies, and tracking cookies, are not essential for functionality but often used for marketing, user behavior tracking, or improving website performance. These usually require explicit user consent due to privacy and security concerns. By limiting permissions, users can minimize unnecessary data collection and potential misuse of their information.

Dealing with Cookie Consent Banners

Different countries and regions have laws and regulations on how websites use cookies. These laws include:

- General Data Protection Regulation (GDPR): Applies to the European Union
- California Consumer Privacy Act (CCPA): Protects California residents
- Personal Information Protection and Electronic Documents Act (PIPEDA): Applies to Canada
- ePrivacy Directive: Applies to the European Union
- Privacy and Electronic Communications Regulations (PECR): Applies to the United Kingdom

Many other countries also have similar cookie laws.

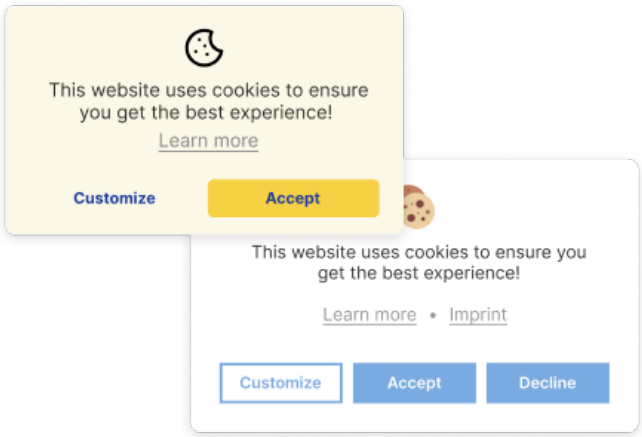

Figure 6: Sample Cookie Consent Banners

Basically, cookie laws require websites to obtain consent from users, before using their cookies. Websites must also record consent and provide proof of it, display a **cookie banner** (Figure 6) on the user's first visit, clearly state what action will grant consent, link to a cookie policy, create and publish a privacy policy.

Here are some simple rules for users to deal with cookie banners effectively and protect their privacy while maintaining a functional web experience:

- Always Read Before Clicking—Take a moment to understand what the cookie banner says, especially if it provides options to manage preferences. Look for phrases like "essential cookies," "analytics cookies," or "advertising cookies" to understand what you're agreeing to.
- Reject Non-Essential Cookies—If the banner gives an option like "Reject All" or "Only Necessary Cookies," select that to minimize tracking. Non-essential cookies (e.g., analytics, advertising) are often used for purposes unrelated to the functionality you need.
- Customize Cookie Settings—Choose "Manage Preferences" or "Customize Settings" when available. Disable categories like "Advertising" or "Marketing" while allowing essential cookies.
- Avoid "Accept All" Unless Necessary—Clicking "Accept All" enables all types of cookies, including trackers and advertising cookies. Use this option only if you trust the site and need its full functionality.

- Look for "Reject All"—Many compliant banners provide a "Reject All" button, often smaller or less prominent than "Accept All." Find and use it to quickly reject non-essential cookies.

- Use Privacy Tools—Install browser extensions such as Privacy Badger (blocking trackers and non-essential cookies automatically), uBlock Origin (blocking ads and tracking scripts). These tools reduce the need to manually manage cookie banners.

- Configure Your Browser Settings—Block third-party cookies globally in your browser settings. Clear cookies regularly or set your browser to delete cookies when you close it. The *Firefox* browser is highly recommended for security and privacy.

- Consider the Website's Purpose—Evaluate the type of website. For trusted sites like banks, it's reasonable to allow essential cookies. For unknown or ad-heavy sites, reject all non-essential cookies to minimize tracking.

- Review the Privacy Policy—If in doubt, check the website's privacy policy for details on how cookies are used. Look for transparency about data collection and sharing practices.

- Use Incognito Mode for One-Time Visits—For websites you don't plan to revisit or be remembered, use your browser's private or incognito mode. This limits cookie storage and prevents long-term tracking.

- Opt-Out of Ad Tracking—Use tools like YourAdChoices to opt out of behavioral advertising cookies across multiple sites.

- Avoid Rushing—If a site pressures you with pop-ups or time-limited offers, pause and ensure you're making informed decisions about cookies.

By following these rules, users can manage cookie banners effectively, minimize unnecessary tracking, and strike a balance between privacy and functionality. Taking small, consistent actions to control cookies can significantly enhance your online privacy.

It is interesting to note that a website remembers your cookie permissions by **using cookies**.

Summary

The stateless nature of the HTTP(S) protocol makes the web efficient and robust. At the same time, it makes remembering important data and information across visits difficult. Web cookies have become an effective and widely used solution. You can say that the cookie mechanism is a *necessary evil* for the web.

Yet, unchecked use of cookies can present privacy and security concerns prompting many countries and regions to enact laws and regulations that require websites to obtain explicit user consent for the nonessential use of cookies. Note that these regulations do not apply to cookies created by browsers on their own initiative.

Dealing with cookies and permissions makes life online more complicated. It highlights the need for computational thinking (CT) to become common sense in the digital age. The idea that CT is literacy will soon become more obvious to everyone.

Figure 7: Why Cookies?

Finally, why **cookies?!** Most think the term originates from the computer programming concept of a "*magic cookie*," which refers to a small piece of data that a program receives and sends back unchanged, essentially acting like a unique identifier. Imagine a program becoming hungry for a cookie and wants it badly like the *cookie monster* (Figure 7) in the PBS kids show *Sesame Street*.