Whatever Does “Accept Cookies” Mean, Really?

by Boran Göher

In the current landscape of the world wide web, any person who spends even the smallest amount of time browsing the internet will definitely run into a prompt requesting their direct consent in order to send and receive cookies between their computer and the server. In other words, the contemporarily notorious “accept cookies” notification. General consensus among regular internet users seems to be that accepting these cookies is not really harmful and accepting them is par for the course. And in the end, you do not have much choice if you want to keep browsing the internet. But should we really be so easygoing about internet cookies or should we be warier of this commonplace practice?

To answer that, we must first understand precisely what a cookie is. For the most part, we can summarize cookies as very small bits of data stored not on the server, but on the user’s computer. They are most commonly used for storing log-in authentications, tracking a user’s movements and history across a website, and keeping track of the specific preference settings of each user. Of course, there are other, less common, usages of cookie technology as well. In short, websites use cookies to check whether you’re logged in, what actions you had taken previously on this website and when, and also to personalize your experience. When used securely and with no malicious intent, cookies are a general boon to one’s internet experience. Still, there are concerns over whatever they can be exploited by malicious-minded people, and these concerns were what led us to see so many pop-ups relating to their use in the first place.

Indeed, one of the reasons that you have to read those long “privacy policy” and “cookie management” texts when you enter a website are concerns over whether cookies are truly safe. One important aspect of this discussion is third-party cookies. Normally, only the site you have entered can send cookies to and receive cookies from your computer and web browser. But sometimes, if the website you entered is streaming content from another website, such as the case with many types of online ads, then that site might potentially be allowed to become a part of the cookie traffic. Those cookies are called third-party cookies and if the same advertisement source is in the two different websites you visit, then the owner of that ad would be able to keep track of your movements on both of those websites. Enlarge the scale and you get advertisers who are able to watch most of your online movements and customize accordingly. This is, of course, perceived as a threat to privacy by many.

Apparently, Europe agrees. The European Union has adopted a directive in 2002 which would limit cookie functions unless the web site was able to produce the data subject’s consent. "the data subject's consent" was defined as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."[1] Similar discussions were also had in the US, where even the NSA was found to be stealthily planting cookies by a privacy enthusiast in the early 2000s.[2] Web browsers also take this issue seriously and are frequently updated with new cookie-related

[1] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[2] https://www.nytimes.com/2005/12/29/us/spy-agency-removes-illegal-tracking-files.html

settings. Most modern browsers allow the user to turn off third-party cookies, turn of cookies entirely for specific sites, disable all cookies and sometimes more.[3] In addition, there are many unofficial addons for these browsers that allow further management of the user's cookies.

In the end, it boils down to a simple question of how much privacy we are willing to give up for convenience. Cookies are definitely an important part of the ease the internet brings into our lives, but they can carry as much penetration power into our privacy as the rest of the internet. The question does not have an easy answer, and it will likely not in the near future. In that case, the best course of action is to be informed and alert. If you trust your government's ability to sufficiently protect your online privacy, you can be more liberal with cookie settings, if you do not have that trust, it is best to be on your toes lest you face unfavorable consequences regarding your privacy.

[3] https://www.nytimes.com/2005/12/29/us/spy-agency-removes-illegal-tracking-files.html