

BIG BROTHER IS WATCHING US!

Necla SÜMER ÖZDEMİR

Deputy Head

External Relations and Competition Advocacy Department

Legal regulations have been made to protect the right to privacy. In these times, when the awareness and request for privacy are emphasized, undertakings may have started to compete with each other over their respect to privacy.

We all use the services provided by the digital world in some way or another. However, what we see while using those services still surprises some and even make their jaws hit the ground, so to speak. We may see the address we checked on the desktop before leaving the house also in our map app on our phones with the notification “Do you want to go here?” even before we get in the car. As soon as we use the internet in a city which we visit the very first time, we see the restaurant ads for that city. A “camp gas cylinder valve”, which we have not search for on the internet and we have not even named before but we mention incidentally while talking with friends, may cover ad spaces when we use the internet afterwards. Web services get to know us inside out through many ways such as the website we sign in with our e-mail address and our open browser, location or microphone access permission.

Siri is spying on us

All happens in the background by means of cookies mainly. Cookie, which we normally associate with delicious food, means a text file placed on users’ devices by websites in the digital world. Cookies are categorized into two, depending on their sources.

First category is the first party cookies which are placed directly by the website a user visits. For instance, the cookies placed by buyclothes.com to run its basic functions are under this category. We add some items to our cart in a shopping website, then we give up and close the website. While we go on our daily life, we see messages in our inbox that reminds us the items in our cart, advising to buy those quickly before they are sold out. When we open the same website again, we see that the same products are waiting for us or we see additional discounts to persuade us to buy the products left in our carts. All those happen thanks to first party cookies.

The second and more widely used category is cookies placed to the website by third parties. Those cookies are mostly used to track users and display personalized ads. Buyclothes.com

receives services from third party service providers for instant messaging function. Similarly, Meta (Facebook), Instagram buttons to share the products you like on social media allow those social media businesses to place cookies on the website as a third party. The user is now being watched on buyclothes.com by not only the website in question but also third party service providers. This is why we see the ads about the clothes we add to the cart on buyclothes.com on other websites too.

Both first party cookies and third party cookies run on website browsers. Cookies are added in the background to each surfing request such as buyclothes.com and the searched website is brought to the user.

Those cookies are mostly used to track users and display personalized ads.

Legal regulations have been made.

Websites have a key role in the functioning of cookies. There are currently different browsers such as Firefox (Mozilla), Edge (Microsoft), Safari (Apple) and Chrome (Google). Legal regulations have been made in many regions from America to Europe, from Europe to Türkiye in order to protect personal data and privacy. At times, some undertakings were punished because they processed personal data without informing users and receiving their consent. Sometimes, undertakings were obliged to put user privacy in the center of their business design even before they have not developed their business. In these times, when the awareness and request for privacy are emphasized, undertakings may have started to compete with each other over their respect to privacy. First Mozilla, then Apple announced that they will not support third party cookies any more. However, the market shares of those undertakings in web browsing market are relatively small, therefore the impact of those decisions is limited.

When it comes to Chrome (Google), its usage rate is about 65% globally. Moreover, Google's activities are not limited to web browsing but cover a wide ecosystem. For instance, Google collects a wide variety and a huge amount of data directly as a first party in many fields such as search engine (Google Search), video sharing, (Youtube), e-mail (Gmail) and cloud (Drive) services. Moreover, Google is a leading advertisement intermediary in the market where data is used in targeted/personalized advertising market. Therefore, unlike the situation for its competitors, it was not possible to cold-shoulder Google's announcement in 2019 that it would end its support to running third party cookies.

Advertising market may be taken over

The advertising sector depends on third party cookies and third party cookies depend on Google. As argued in the investigation by the United Kingdom Competition Authority, in the absence of the third party data collected by third party cookies, in terms of the first party data, concerns have arisen that a very small number of companies such as Google and Meta will dominate online advertising sector.

Of course, how users perceive those is also important. Some users prefer seeing personalized ads rather than irrelevant ads and even finds it useful. On the other hand, some users are sensitive about privacy. This different attitude is reflected in the reactions of players in the online advertising sector (advertisers, publishers, intermediaries, etc.) to browsers ending their support to the functioning of third party cookies. Some people foresee that online advertising will be more compliant with legal regulations concerning personal data in this way. Some are more anxious about the business models awaiting in the new world.

The good news is that Google is discussing the alternatives for the new era publicly on the forums with the shareholders and working jointly to develop a model. With the latest version of Google's announcement after the updates, this model is expected to be in practice in the second half of 2024.

How the user privacy, the functioning of online advertising sector and the protection of competition will be balanced as well as what kind of a model will be developed, remain as a question to be answered in the future.