弁護士法人中央総合法律事務所
CHUO SOGO LAW OFFICE, P. C.

Cookies under Japanese Law

August 10, 2022
Yo Kashibuchi, Attorney
E-mail: kashibuchi_y@clo.gr.jp

I. Introduction

On April 1, 2022, two sets of amendments (sometimes referred to as “cookie restrictions”) to the Act on the Protection of Personal Information (the “Act”) went into effect, giving rise to questions of how to deal with cookies. For example, “When I open a website,” someone would ask, “I often see a pop-up message appearing on the screen and asking me whether to accept cookies. Should my firm also introduce similar pop-ups on its website in the wake of these amendments?”

For most business operators the answer to such questions is no – they are not required to take such steps as far as the Act is concerned. Nevertheless, a prudent policy would be to look at these questions and make decisions on a case-by case basis.

This article offers an outline of regulations concerning Personally Referable Information[1], focusing mainly on the relationship between cookies and the Act.

II. What are cookies?[2]

1. How Internet works

To begin with, it may be essential to know how the Internet works, including some computer terminologies, to understand what cookies are.

Let's assume that you are shopping on Amazon’s website to purchase some fitness gear with your own computer, as illustrated in Figure 1. To do so, you will likely connect to Amazon’s website by using Microsoft Edge or Chrome, programs on your computer which are called **web browsers**. On the other hand, devices called **web servers**[3] play a role of communicating with web browsers by sending out content (in this case, the content to be

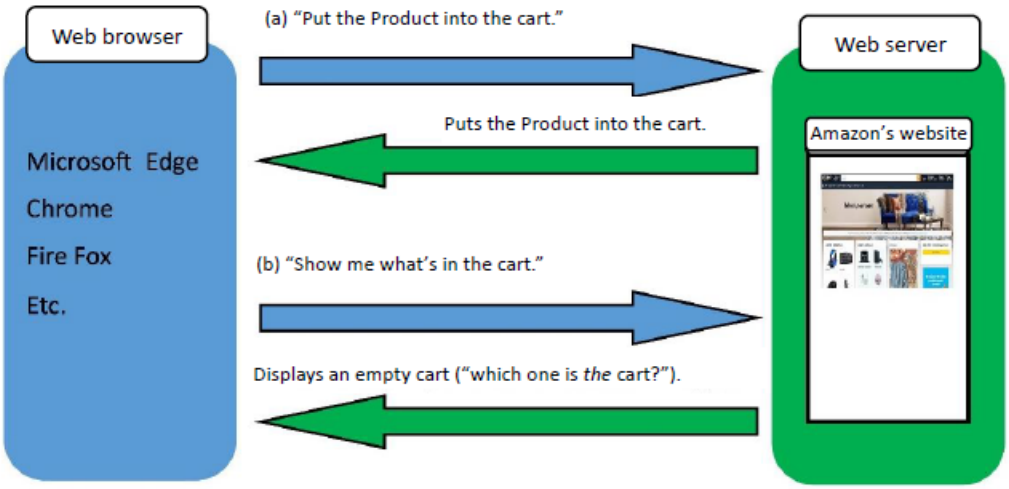
[1]"Personally Referable Information" is defined as "information concerning a living individual that does not fall within any of the categories of Personal Information, Pseudonymized Information or Anonymized Information" (the Act, Art. 2, para.7). For example, online browsing history, location and cookies that are not associated with a person’s name are considered to fall within the category of Personally Referable Information (*Q&A: Revision 2020 of the Act on the Protection of Personal Information*, Q51).

[2]Sources of reference for the explanations offered in this article are: *Illustrated Guide: All the Basics You Need to Know to Understand Web Technologies* (Author: Kyohei Kobayashi and Akira Sakamoto; Supervisor: Takuro Sasaki; SB Creative Corp., 2017) (the "Basics"), and the translated (Japanese) version of *Understanding the Digital World: What You Need to Know about Computers, the Internet, Privacy, and Security* (second edition; Brian W. Kernighan, Nikkei BP Marketing, Inc., 2020) (the "Handbook").

[3]Computer devices performing a role of providing information or services online are collectively referred to as “servers.” Servers are used for various purposes, and those providing websites are specifically called “web servers.” (Basics, page 34)

displayed as Amazon's website) to them.

Figure 1.



As a basic rule, each communication process between a web browser and a web server takes place as a single, complete process without being affected by any preceding communication process.

Let's say, in the foregoing example of shopping on Amazon's website, you searched for your favorite fitness gear and put one particular product ("Product") into the cart (process a), and then, after briefly searching for other similar products, clicked on the cart icon (process b) to proceed to the purchasing step, having made your final decision to buy the Product. If the above-mentioned basic rule is applied as it is, process (a) should not have any effect on process (b) because they are each an individual process between the browser and the web server. As a result, you will never find your Product in the cart by the time you finally make up your mind to purchase it.

This is not the way you want to shop. One possible solution could be to let the web server remember process (a), but considering the fact that web servers are being accessed by an enormous number of web browsers, storing all the processes made between the web server and web browsers might not be entirely feasible.

The mechanism we know today as "cookies" was devised to tackle such inconvenience.

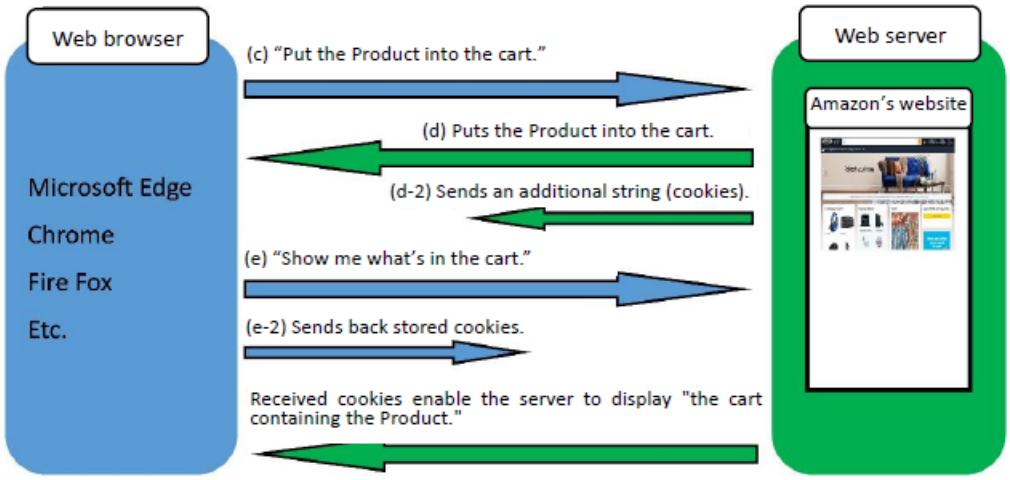
2. Example of cookies' roles

Let's take a look at Figure 2 below. In this case, once your web browser sends a request to

Amazon's web server to put the Product into the cart (process c), the web server will send back the required content in response to the received request (process d) to the web browser, and at the same time, along with the requested content, the web server will also send an additional sequence of characters (a "string") to the browser where the string will be stored (process d-2). This additional string which is being sent to the web browser is referred to as **cookies**.[4]

In most cases, web servers incorporate into cookies an ID that enables identification of each browser. Also, a certain range of information, such as login status, items contained in the cart and user settings, will be kept on the web server's side as a set of information associated with each ID.[5]

Figure 2.



If, subsequently, your web browser sends another request ("show me what's in the cart") (process e) to the same web server, the cookies stored in your web browser will be sent back to the web server at once (process e-2). By receiving the cookies back from the web browser in this way, the web server can recall the relevant interactions that have been completed until then because, as described above, the web server keeps the relevant information associated with the ID embedded in the received cookies.

As seen above, cookies are just strings designed to be sent back after being stored in web

[4]In actual cases, cookies will be stored on web browsers earlier in time (e.g., when the home page of Amazon's website is accessed by the browser). The timeline shown in this article is deliberately simplified for the sake of making a coherent explanation.
[5]Handbook, page 356.

browsers, and the only server to which cookies are sent back to is the one they were originally sent from.[6] In our shopping on Amazon example, the communication process (e), which is now based on process (c), has become possible due to cookies exchanged between your web browser and Amazon's web server.[7]

3. First-party cookies and third-party cookies

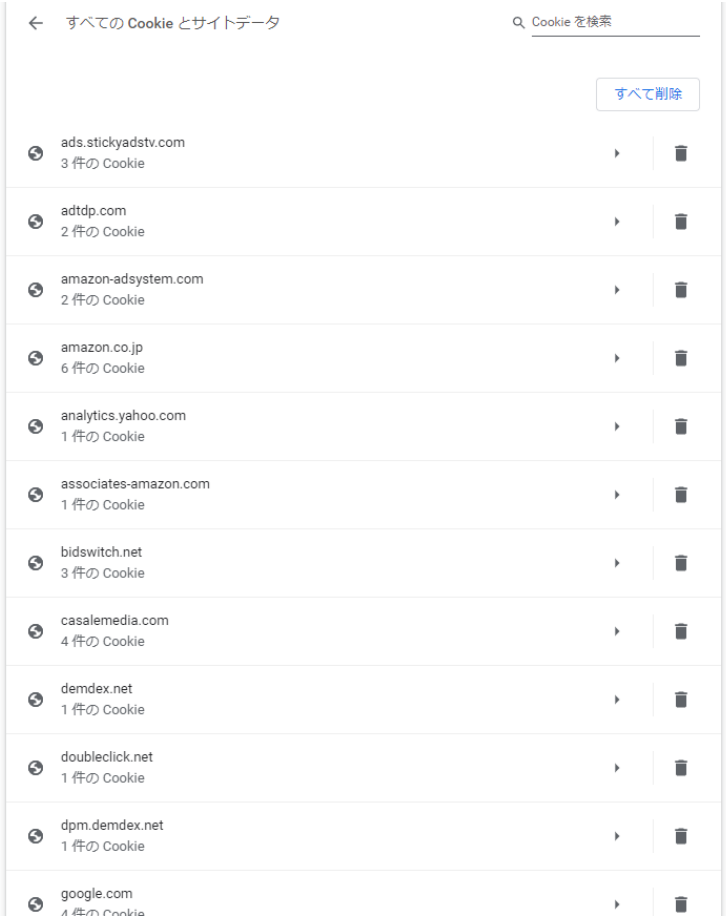
When shopping on Amazon's website, the cookies sent from Amazon's web server (amazon.co.jp[8]) are being stored in your web browser as a result of accessing Amazon's server. These cookies stored in your web browser, which are sent directly from the content provider you are accessing, are called **first-party cookies**. In some cases, as illustrated above, first-party cookies occupy a vital role in making effective use of the content.

However, in some cases where, in the context of our Amazon example you are accessing Amazon's web server, your web browser stores cookies sent from not Amazon's but a third party's server (thirparty.com). Such cookies, which are not sent from the provider of the content being accessed but from some other entity, are called **third-party cookies**. Third-party cookies are used primarily for targeted advertising.

Shown below as Figure 3 is part of cookies stored in my Chrome browser, which were confirmed immediately after I accessed the home page of Amazon's website by using the same Chrome with all cookies deleted beforehand. Among the list of the stored cookies, those not from Amazon's web server (amazon.co.jp) are the third-party cookies.

[6]Handbook, page 356.
[7]There are two types of cookies: those with and without a predetermined lifetime. Those with predetermined lifetime will be removed from the web browser when such lifetime ends, while the others will be removed from the web browser once the browser is closed. (Basics, page 74)
[8]Strings often seen as "xxxx.com" or "xxxx.co.jp" are being used as strings for identifying and accessing intended online servers, which is called "domains." (Basics, page 42)

Figure 3.



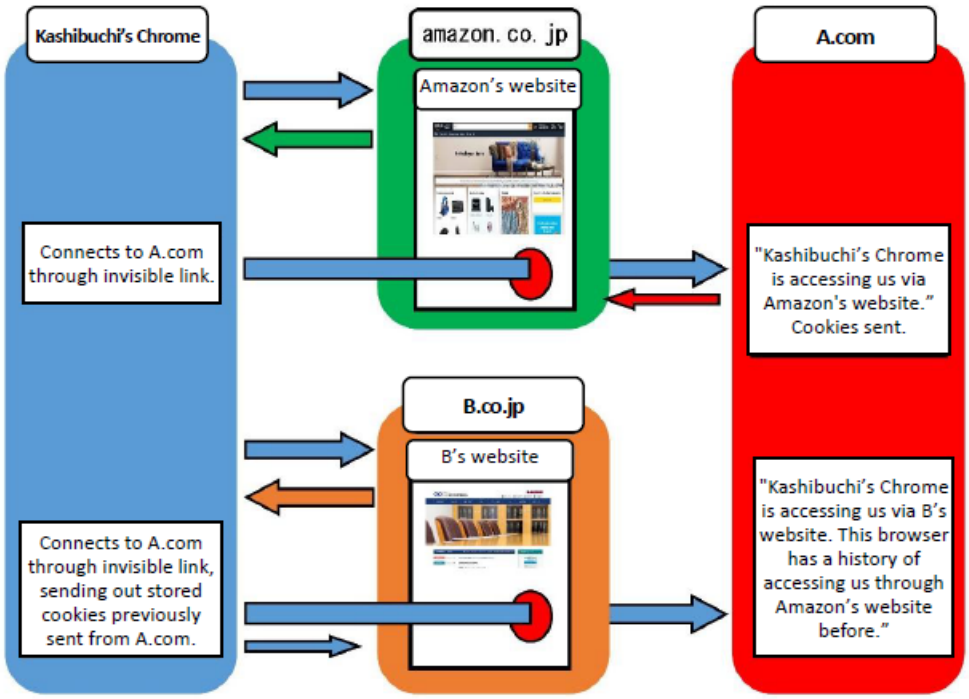
What is the purpose of these third-party cookies stored on my computer?

Some websites contain one or more embedded links, which could be either visible or invisible, leading to other websites. If a website has an invisible link, the link will be followed at the same time when the website is accessed. In other words, when I open Amazon's home page, my Chrome is also being connected to the server of some other parties other than Amazon (as shown in Figure 3), for example, a third party "A". During such a process, A's server can learn that my Chrome is being connected to Amazon's home page, and can send its third-party cookies to my Chrome.

If, by using the same Chrome, I open a website of another company, say company "B", and its website has an invisible link that leads to A's server, then my Chrome will once again be connected to A's server, sending out the cookies previously received from A. This enables A's

server to learn that my Chrome was once connected to Amazon's home page and is now accessing B's website[9] (see Figure 4 illustrating such a flow).

Figure 4.



By repeating such a flow, A's server (A.com) will eventually be able to grasp each browser's (in this case, my Chrome's) preferences. Targeted advertising is a method of advertising that utilizes information obtained in this way to display ads that are likely to suit each user's preferences. Companies like A in our scenario are called DMP (Data Management Platform) vendors.

III. Cookies and the Act

Some restrictions under the Act apply to cases where "any Personally Referable Information . . . is expected to be obtained as Personal Data by a third party" (the Act, Art. 31, para. 1). Because of the fact that, as described in footnote 1, Personally Referable Information includes cookies, it should be examined on each occasion of providing cookies to a third party whether such provision could be subject to restrictions set forth in Article 31(1) of the Act.

That said, as described in Section II, cookies are mere strings sent from servers to web browsers which are designed to be stored in each browser and then sent back to the server from

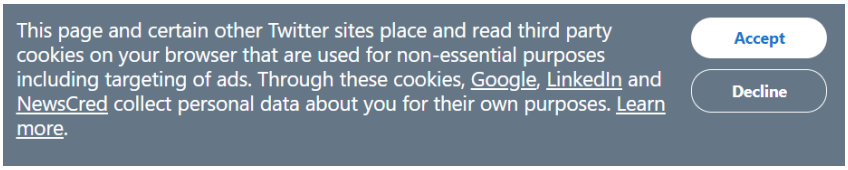
[9]Handbook, pages from 407 to 412.

which they were originally sent. The act of exchanging cookies in such a way is unlikely to be seen as an instance of "providing cookies to a third party" as long as they are being exchanged in an ordinary way, even when the cookies exchanged are third-party cookies as those seen in the example discussed above.[10]

Therefore, as far as ordinary exchanges of cookies are concerned, it is quite unlikely that such use of cookies will be subject to the restrictions set forth in Article 31(1) of the Act. However, in some cases, for example, when a DMP vendor provides advertisers with information it has gathered for the purpose of targeted advertising, an examination of whether it would be subject to the regulations may be required.

IV. About pop-ups asking whether to accept cookies

Below is an example of a pop-up often seen on websites in recent years.



(Source: https://about.twitter.com/en)

As discussed in Section III, presenting this sort of a pop-up message may not necessarily be required under the Act. Moreover, cookies are considered to have certain problems because, as described above, third-party cookies can be used to collect a variety of information, and such information may potentially be used for identifying individuals through analyses. As seen in the EU's General Data Protection Regulation (GDPR), which includes cookies in its scope of application, restrictions on cookies are becoming increasingly strict internationally. Furthermore, new mechanisms aimed at replacing cookies are currently under development. For example, Apple's Safari has already introduced a feature to prevent third-party cookies from functioning, and it has been announced that Google Chrome will phase out and eventually discontinue using third-party cookies in a not-so-distant future[11].

To address some of these issues, Japan Interactive Advertising Association (JIAA), a general incorporated association comprised of 289 (as of July 29, 2022) companies involved in online advertising business (e.g. media providers and advertising companies), is working to promote a healthy development of, and improvement of public confidence in online

[10]Refer to Q8-10 of *Q&A with respect to "Guidelines on the Act on the Protection of Personal Information"* (Personal Information Protection Commission, updated on May 26, 2022).
[11]https://blog.google/products/chrome/update-testing-privacy-sandbox-web/. Although the timing of discontinuation was originally scheduled to be by 2022, it was rescheduled for the latter half of 2024 on July 27 of 2022.

advertising. In order to ensure that a clear explanation of how to handle gathered data and opportunities for opt-out is always available to users, JIAA has formulated the "Privacy Policy Guidelines,"[12] which has been introducing regulations as strict as those concerning Personal Information stipulated in the Act but with a wider range of information, including information categorized as Personally Referable Information (i.e. excluded from Personal Information) according to the Act, together with more detailed provisions set out in the "Guidelines on Behavioral Targeting Advertisement."[13]

In summary, it appears that companies that have opted to introduce pop-ups such as those discussed in this article were under no legal requirements to do so. Rather they seem to have made their own judgment to display such pop-ups in order to stay on top of the prevailing and growing trend among current website owners.

[12] https://www.jiaa.org/wp-content/uploads/2019/11/JIAA_PPguideline.pdf
[13] https://www.jiaa.org/wp-content/uploads/2019/11/JIAA_BTAguideline.pdf