THAT’S HOW THE COOKIE CRUMBLES…

Category: Commercial Law,Media and OTT,Privacy Law, Infosec, and POPIA,Technology Law
written by Yashoda Rajoo | January 9, 2019

No, I don’t mean those midnight snacks you’ve been sneaking. Cookies are small files which are stored on a user’s computer. They are designed to hold a small amount of data specific to a particular user and website that can be accessed either by the web server or the client computer. This allows the server to deliver a page tailored to the user. The page can contain some script which is aware of the data in the cookie and can carry information from one visit of the website to the next.

Each cookie is basically a small table containing pairs of (*key, data*) values – for example (*firstname, John*) (*lastname, Smith*). Once the cookie has been read by the code on the server or client computer, the data can be retrieved and used to adapt the web page appropriately.

Cookies are a convenient way to carry information from one session on a website to another, or between sessions on related websites, without having to burden a server machine with massive amounts of data storage. The purpose of cookies is to help the website keep track of your visits and activity, and this isn’t always a bad thing. Many online retailers use cookies to keep track of the items in a user’s shopping cart as they explore the site. Without cookies, your shopping cart would reset every time you clicked a new link on the site. That would make it impossible to buy anything online! A website might also use cookies to keep a record of your most recent visit or to record your login information. This is useful to store passwords on commonly used sites, or simply to know what you have visited or downloaded in the past.

Writing data to a cookie is usually done when a new webpage is loaded – for example after you press the ‘submit’ button, the data handling page is responsible for storing the values in a cookie. Most browsers have a configuration screen which allows you to see what cookies have been stored on the computer, and delete them if you need to. If you choose to disable cookies then the write operation will fail, and sites which rely on the cookie will usually require you to re-enter the information that would have been stored in the cookie.

Cookies aren’t really a threat to privacy since they can only be used to store information that the user has volunteered or that the web server already has. Under normal circumstances, cookies cannot transfer viruses or malware to your computer. The data in a cookie doesn’t change when it travels back and forth, it has no way to affect how your computer runs. However, some viruses and malware may be disguised as cookies. “Supercookies” can be a potential security concern, and many browsers offer a way to block them. Third-party tracking cookies can follow you around the Internet and report back to marketing and other companies telling them where you've been online A supercookie is a kind of tracking cookie. Supercookies can be used to collect a wide array of data on your browsing habits including what websites you visit and when you visit them. Supercookies can also access information collected by traditional tracking cookies — including login information, cached images and files and plug-in data — and store that information even after the traditional cookie has been deleted.

Banning all cookies makes some websites difficult or impossible to navigate. A setting that controls or limits third-party and tracking cookies can help protect your privacy while still making it possible to game, shop online, or do your banking.