Are Cookies good or bad for you?

John Wiseman, Privacy in Digital Economy Working Group

Cookies, tiny virtual crumbs of your online activity - a sweet treat for tech. Why does something so innocent sound so contentious?

Cookies are small data 'packages' that are stored on your browser when you visit websites. These seemingly innocuous additions perform some helpful functions such as remembering your preferences for that website, storing purchased items in baskets and wish lists and maintaining your log in status to make it simpler and quicker next time you visit that website. Whilst they do perform some functions that can be helpful, are you aware of the price you may be paying for this service?

When it comes to our own personal privacy the use of cookies and the data collection behind them has been debated for a number of years. Typically focus has been upon the type of and volume of personal data collected, the transparency of collection (i.e., do you know what is being collected), and that this data can potentially be sold/shared with unspecified third parties, who may be unconnected to the original purpose of your search.

Why should this be of concern?

Over time, through the use of cookies, enough personal data can be gathered about you to build a comprehensive picture of your digital footprint through your online activities, which can then be linked to your identity. At face value you may think 'why does it concern me if I get more adverts for handbags, I love handbags?', but consider the cumulative effect of this. Data collected often include all browsing activity, including potentially identifying your political/societal tendencies from articles viewed/videos watched, opinions expressed online and the use of various Social Media tools. This continual collection of data over time can enable a comprehensive picture being built, which can then be leveraged for targeted marketing or possibly more nefarious purposes, such as influencing your political choices.

Companies who collect/purchase data collected via cookies, would be able to focus advertising and initiate a continual presentation of similar content, potentially creating an echo chamber of views and opinions presented to you. Arguably this has been seen with the visible explosion of conflicting views and (so called) 'facts' presented through social media in the 2021 US elections, allegedly magnified by Russian interference via deliberate 'nudging' of individuals views. Presenting extreme political views without balanced information is one of the factors blamed for the rising polarisation and left and right wing tensions in the US political sphere. Added to this the fact that Facebook alone has collected personal data on over 3 Billion private individuals[1] globally through its use of accounts/tracking web/app activities, not all of whom have signed up and created their own Facebook profiles, but who may have 'shadow' profiles created of them. The level of awareness of your online activities by corporations could easily be used to nudge your views or cement your opinions for the benefit of third parties, potentially without you even realising.

In some jurisdictions (including the European Union), Websites and Apps are now required to obtain your consent to use of cookies (via pop ups and your browser settings), but how many of us read the small print, and know whether our data is being sold on, and if so, to whom? Do you reject all cookies, accept required cookies, or accept all cookies? Do you know they are and the impact of the differences? There is one UK daily paper which requests permission to share your browsing action with over 1,300 of their 'partners'!

Some companies have recognised this concern and have taken further steps to block the use of third-party cookies. Google is rolling out an upgrade to prevent the use of third-party cookies during 2024, and Apple (Safari) and Firefox have already implemented the same restrictions for a few years now. When a tech company like Apple roll something like this out, they clearly are responding to consumer concerns and realise they will lose market share and revenue if they continue to ignore privacy concerns. This does not stop them from collecting data via cookies for their own purposes however, so perhaps whilst addressing some privacy

[1] Facebook MAU worldwide 2023 | Statista

concerns on the one hand, they are further cementing their corner of the market for this valuable data collection to 'trusted' browsers.

What can you do to minimise impact?

- Review your browser settings on a regular basis to block or restrict the collection of cookies, but also by clearing cookies stored on a regular basis
- Consider using some browser plug-ins to prevent online tracking or manage cookies, for example Privacy Badger, uBlock Origin, Click&Clean, or Edit This Cookie.
- Consider changing the browser you use, especially if they continue to allow third party cookies.
- When the pop up appears asking for consent to the use of cookies, decline or restrict your acceptance to those required for the operation of the website.
- Stay informed! Keep up to date generally on the changes around the use of cookies, and on a wider basis, the potential use/misuse of your personal data.