Cookies and online advertising: an ongoing changing scenario

April 29, 2020

Cookies are the main technologies that enable effective online targeted advertising (for more information on advertising in the social media environment and AdTech, see our previous bites here and here). These tracking technologies are still regulated by the ePrivacy Directive, which will soon be replaced by the ePrivacy Regulation (currently under discussion within the Council of the European Union). The new provisions will need to take into account that some important technology companies are already phasing out third-party cookies from their browsers.

What are cookies and how are they regulated?

Cookies are small pieces of information, normally consisting of letters and numbers, stored on a device such as a PC, a mobile device or any other device that can store information, including 'Internet of Things' (IoT) devices that connect to the Internet. This technology is used for several purposes, e.g. to remember previous interactions with a website, to identify users when they log into an online account (e.g. banking account) and to help web pages to load faster and to route information over a network. It is also used to analyze traffic to a website and track users' browsing behaviour. Consequently, on the basis of the function served, cookies can store personal data, such as an IP address, a username, a unique identifier or an email address, but it may also contain other (potentially) non-personal data such as language settings or information about the type of device a person is using to browse the site. Moreover, cookies may contain tracking IDs such as advertising IDs and user IDs (with regards to apps, the so-called IDSA). Finally, it is important to underline that cookies can be either installed by first parties or third parties: First-party cookies are set by the domain of the website that the user is visiting (i.e. the host domain), while third-party cookies are set by a domain other than the one the user is visiting (i.e. a domain other than the one that it can be seen in the address bar). First-party cookies are most commonly used by webpage owners to save details such as the users' passwords in order to facilitate future access to their accounts, while third-party cookies are used primarily for retargeted advertising.

There are many types of cookies: From the well-known browser or http cookies to other lesser-known typologies of tracking technologies such as local storage objects (LSOs) or "flash" cookies, software development kits (SDKs), pixel trackers (or pixel gifs), "like" buttons and social sharing tools, and device fingerprinting technologies. All these different tools fall within the scope of the ePrivacy Directive, which was adopted in 2002 with the aim of protecting the privacy of individuals during their electronic communications. Computers and mobile phones are users' terminal equipment for electronic communications networks and, together with any information stored on such equipment, are considered part of the private sphere of users and are hence protected. Art. 5(3) of the ePrivacy Directive, which requires the consent of users in order to store any information on an individual's terminal equipment or to gain access to the information stored, aims to protect internet users from the risk of having information placed or accessed on their devices without their consent or awareness, potentially interfering with the confidentiality of their communications. However, Art. 5(3) provides for a consent exemption in case of "technical" cookies, i.e. where the storage of or access to the information is made for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or if strictly necessary in order to provide an information society service

explicitly requested by the user. The provisions of the ePrivacy Directive have been transposed by all EU member states in national laws. With regards to Italy, the Legislative Decree n.196/2003 ("**Italian Privacy Code**") was adopted to implement both Directive 2002/58/CE (ePrivacy Directive) and Directive 95/46/EC ("**Privacy Directive**").

Moreover, as remarked by the European Court of Justice in the Planet49 judgment, Art. 5(3) of the ePrivacy Directive applies when any information is stored on or accessed from the device, regardless of whether the information constitutes personal data. This aspect becomes relevant in the first case (when the information stored or accessed is e.g. an identifier that may be used to identify a user and to profile or target advertise him/her). Such a processing operation is regulated not just by the ePrivacy Directive's provisions but also by the rules set out by the new General Data Protection Regulation ("**GDPR**"). In fact online identifiers are explicitly considered personal data by Art. 4(1) of the GDPR. Therefore, the storage of or access to such information must comply with both the ePrivacy Directive, which requires to obtain the consent of the user, and the GDPR, which provides the requirements for a valid consent, i.e. "freely given, specific, informed and unambiguous".

Moreover, as Recital 17 of the ePrivacy Directive makes reference to the meaning and definition of "consent" as provided by the Privacy Directive, now replaced by the GDPR, it is clear that the requirements for a valid consent as provided by GDPR should apply. Hence, the consent must be not only freely given, specific and informed, as requested by the Privacy Directive, but also unambiguous, i.e. expressed with a statement or a clear affirmative action signifies agreement to the processing of personal data.

Which role do cookies play for the online advertising industry?

Cookies can be related to advertising. In particular, thanks to the use of cookies-markers, website users can be monitored with reference to where they go and what they do: they are "tracked" through the dynamic IP addresses of their device and other related information (such as user ID, user agents, etc.). Consequently, by surfing the Internet, clicking a banner, selecting an item or opening a page, the user gets analyzed, and after his/her preferences are monitored again in the future the user will be defined as belonging to a specific cluster of individuals, as defined by the online advertising product-chain (including publishers, media agencies / centers, web monitoring service providers, etc.). This enables profiled advertising to be addressed to each user.

This is the reason why cookies are considered the key tool behind online advertising. However, while first-party cookies are most commonly used by webpage owners to save details such as the users passwords in order to facilitate the future access to their accounts, third-party cookies are used primarily for retargeted advertising. Therefore, for advertising purposes, specific consent of web site visitors is required.

In order to better clarify the practical modalities for obtaining such approval, many European data protection authorities have released specific guidelines on cookies and other tracking technologies, lastly the Irish Data Protection Commission and the Belgian Belgian Data Protection Authority (you can find the full text of their guidelines here and here). For instance, the Italian data protection authority ("Garante per la protezione dei dati personali, "**Garante**"), on its guidance regarding "Simplified arrangements to provide information and obtain consent regarding cookies" published in 2014 (see the full text here, also available in English), clarified that the owner of the website (publisher), allowing the setting of third-party cookies for marketing and profiling purposes, despite acting as a technical intermediary between third parties and users has the duty to obtain the users' consent and to make reference in its cookie policy of the third parties.

End of an era for Internet ads?

For many years third-party cookies have represented the cornerstone of internet advertising. However, significant changes may occur. In fact, Google recently announced that it will phase them out from the Chrome browser. Following that statement, Apple announced on March 24, 2020, a major system update to iOS Intelligent Tracking

Prevention (ITP). This feature allows Safari to block the installation of all kinds of third-party cookies. Through the new update, Safari now promotes a default setting able to prevent any advertiser or website from following users on the Internet through common tracking technologies. It will be important to investigate the functioning of such new features and the further clarifications that will be provided.

In light of the above, in order to address the losses that the online advertising industry may suffer from the phasing out of third-party cookies, the Interactive Advertising Bureau (IAB) announced the launch of the ReArc Project on the occasion of its Annual Leadership Meeting. The initiative aims to mitigate the negative consequences of the loss of third-party cookies by allowing targeted advertising through an identifier that can be directly managed by users. However, the IAB specified that it will not pursue the creation of an universal identifier, but commit to (i) collect information on existing practices among first parties for the use of address identifiers provided, by consent, by consumers, (ii) encourage the industry to work together to ensure responsible use of identifiers provided by consumers, while fully respecting their privacy, and (iii) develop strict technical standards and guidelines for companies that collect and use such identifiers.

Do you have more questions, or do you want to share your thoughts on this article? Contact our Dentons Italy TMT Team at tmtbites.italy@dentons.com, and do not forget to sign up to our TMT Bites Newsletter!

This article has been co-authored by Ilaria Boschi (ilaria.boschi@dentons.com)

Your Key Contacts

Giangiacomo Olivi
Partner, Milan
D +39 02 726 268 00
M +39 344 27 62 550
giangiacomo.olivi@dentons.com

Fabia Cairoli
Associate, Milan
D +39 02 726 268 00
M + 39 347 28 61 698
fabia.cairoli@dentons.com