The end of third-party cookies

Coton, Fanny; Ruelle, Victoria

Published in:
Time to reshape the digital society

Publication date:
2021

Document Version
le PDF de l'éditeur

CHAPTER 2
The end of third-party cookies: nothing but smoke and mirrors if the RTB winner takes it all?

Fanny COTON[1]

et

Victoria RUELLE[2]

Introduction

Cookies are small text files that can be deposited on the users' computer when they visit websites. These files contain different information about users or at least about their online behavior. It may be the language in which the users wish the web pages to be displayed, their login and password (so that they do not have to systematically type them), the products left in a shopping cart despite their disconnection, etc.

Cookies appeared in the 90's in order to give websites a memory that the HTTP protocol did not provide in itself.[3] The goal is for the website to identify the cookie when the user visits the same website later on and to reflect the user's previous choices on the new navigation session. In view of these examples, cookies seem to facilitate the navigation of the Internet user.

However, this mechanism often takes place without the users' knowledge, as they do not realize that their data are being manipulated.

In addition, cookies can also serve other purposes that go beyond what the user might expect. Firstly, and since cookies can identify users when they log on or log off a web page, it becomes possible to track them

[1] Partner, Lexing Belgium.

[2] Lawyer, Lexing Belgium, Researcher CRIDS (UNamur).

[3] M. VEALE, F. ZUIDERVEEN BORGESIUS, "Adtech and Real-Time Bidding under European Data Protection Law", *German Law Journal*, April 1, 2021, https://osf.io/preprints/socarxiv/wg8fq/.

throughout their web browsing on different websites. Secondly, cookies allow a massive collection of data, making it possible to deduce additional information about the user and to establish a precise profile. Due to the combination of tracking and profiling, cookies are the most widely used way to display targeted advertising to this date. There may be some rapid changes to this situation as some players in the digital world are moving away from the use of cookies – thus developing alternatives – and because the European legislator plans to adopt a new Regulation applicable to cookies.

Knowing the audience is one thing, finding advertisers who want to pay to display an ad to the profiled users is another. There comes *real time bidding* ("RTB"). It consists of an instantaneous bidding system for advertising spaces that allows to match user profiles with the advertisers' target audiences. RTB is nowadays widely used in the field of online advertising and is primarily based on cookies.

This paper proposes to address the issues raised by third-party cookies and their successors (title I), as well as the legality of the RTB system (title II).

I. Cookies and Their Heirs

A. Legislative Frame

1. E-Privacy Directive and GDPR

Article 5 of the e-Privacy Directive[4] specifically deals with cookies and similar tracking devices installed on a user's browser. In general terms, it states that the use of cookies requires the user's consent, with some exceptions.[5]

Cookies make it possible to collect different information about the user: IP address, searches made, online transactions, browsing history, etc. The use of cookies thus consists of processing personal data. General

[4] Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ("e-Privacy Directive"), *O.J.*, L. 201, July 31, 2002, pp. 37–47, Art. 5.

[5] Article 5, e-Privacy Directive provides that: "This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user".

data protection legislation, *i.e.* the GDPR,[6] consequently applies. In the well-known "Planet 49" decision,[7] the CJEU confirmed that the consent referred to in the e-Privacy Directive is the same as the consent required by the GDPR[8] as a basis for lawful processing.[9] Therefore, the use of cookies requires a prior, informed, specific, free, and unambiguous consent of the person.[10] [11]

2. Future E-Privacy Regulation

In 2017, a first proposal for a new e-Privacy Regulation ("e-Privacy Regulation 2017 Proposal") to replace the Directive was published.[12] By introducing a Regulation proposal, the EU wanted to ensure a harmonized regime among all Member States. After a long and tumultuous legislative process, during which each presidency successively proposed a draft for the e-Privacy Regulation,[13] the Portuguese presidency finally succeeded

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR"), *O.J.*, L.119, May 4, 2016, pp. 1–88.

[7] CJEU, *Bundesverband der Verbraucherzentralen und Verbraucherverbände-Verbraucherzentrale Bundesverband eV v. Planet49 GmbH*, case "Planet49", October 1, 2019, C-673/17, ECLI:EU:C:2019:801.

[8] Art. 6, GDPR.

[9] About the coordination between the GDPR and the e-Privacy Directive, see C. Etteldorf, "EDPB on the Interplay between the ePrivacy Directive and the GDPR", *EDPL reports*, 2/2019, pp. 224-231, https://doi.org/10.21552/edpl/2019/2/12; See also EDPB, "Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities", March 12, 2019, https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf.

[10] Art. 7, GDPR.

[11] The GDPR also applies in its other provisions including the requirements in terms of profiling that is made with the data collected through cookies. Regarding this question, see P. Limbree and F. Coton, "Les données, des armes de déduction massive (données massives, recherche scientifique, profilage et décision automatisée à l'ère du Règlement Général sur la Protection des Données)", in A. Cassart (dir.), *FinTech, LegalTech, MedTech… Quels défis juridiques se cachent derrière les MachinTech?*, Larcier, Louvain-la-Neuve, 2018, pp. 9-80.

[12] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC ("e-Privacy Regulation 2017 Proposal"), Brussels, January 10, 2021, COM/2017/010 final – 2017/0003,https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010&qid=1623856330187.

[13] After the initial draft proposed by the EU Commission, other drafts were proposed by the Estonian, Bulgarian, Austrian, Romanian, Finnish, Croatian, and German Council presidencies. (CMS law, "E-Privacy – European regulation on privacy and electronic communications", May 10, 2021, https://cms.law/en/deu/insight/e-privacy).

in convincing the other Member States to agree to its text.[14] Therefore, negotiations on the basis of this latest text ("e-Privacy Regulation 2021 Proposal")[15] are about to begin. However, if adopted, it will not apply before 2023 due to the duration of the legislative process as well as the transitional period set forth by the 2021 Proposal itself.[16] [17]

Article 8 of the 2021 Proposal limits the use of end-users' "terminal equipment information to specific conditions such as the necessity for the sole purpose of providing an electronic communication service or another service specifically requested by the end-user, audience measuring, software updates, etc.".[18]

Among the Article 8 exceptions, the processing of cookies is also lawful if the user gave his/her/their consent. When it comes to online advertising, there is no doubt that consent will continue being the only legitimate ground to process the end user's data under the e-Privacy Regulation, as it is the case under the Directive.[19]

The 2017 Proposal broke new ground when it placed obligations on browsers, deemed to possess a gatekeeper position allowing them to assist the data subjects who wish to control their data.[20] This implied a "do not track me" setting in the browser, comparable with the "do not call

[14] Council of the EU, "Confidentiality of electronic communications: Council agrees its position on ePrivacy rules", *Press release*, February 10, 2021, https://www.consilium.europa.eu/en/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/.

[15] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC ("e-Privacy Regulation 2021 Proposal"), Brussels, February 10, 2021, 6087/21, https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf.

[16] Art. 29, § 2, e-Privacy Regulation 2021 Proposal states that it will apply from 24 months from the date of its entry into force. However, Article 27 sets the repeal of the e-Privacy Directive on August 1, 2022.

[17] Originally, the new Regulation was supposed to come into force simultaneously with the GDPR. However, some points, including the rules applicable to cookies, have raised some disagreements, which explains why it is still not adopted today: C. Etteldorf, "A New Wind in the Sails of the EU ePrivacy-Regulation or Hot Air Only? On an Updated Input from the Council of the EU under German Presidency", *EDPL Reports*, 2/2020, p. 568.

[18] Art. 8, e-Privacy Regulation 2021 Proposal.

[19] Art. 6.1.h), e-Privacy Regulation 2021 Proposal about the conditions upon which one can use data obtained thanks to cookies without consent for compatible purpose expressly states that this does not apply if the data is used for profiling.

[20] Recital 22, e-Privacy Regulation 2017 Proposal: "this Regulation should provide for the possibility to express consent by using the appropriate settings of a browser or other application".

me" list for commercial calls.[21] Those considerations were embodied in Article 9 of the 2017 Proposal[22] whose idea is now replicated in the new Recital 20a[23] and Article 4a of the 2021 Proposal. Those provisions state that the software settings must allow users to express their preferences regarding cookies.[24]

Furthermore, Article 4.a of the 2021 draft states that "end-users (…) shall be reminded of the possibility to withdraw their consent at periodic intervals of no longer that 12 months",[25] whereas the 2017 Proposal indicated 6 months.[26]

Finally, in order to ensure the enforcement of these measures, an authority must monitor the compliance with these new obligations. This

[21] Initially, the setting of the browser will be set to accept cookies and users will have to change this themselves. This seems to be in contradiction with the principle of privacy by default provided for by the GDPR in its Article 25. Privacy by default would require the setting to be defined as refusing cookies. It is only if users activate, by a positive act, the use of cookies that they mark their explicit consent. However, the browsing setting is not supposed to be a tool to collect consent but rather a tool offered to the data subjects to have a better control of their data.

[22] Art. 9, e-Privacy Regulation 2017 Proposal: "consent may be expressed by using the appropriate technical settings of a software application enabling access to the Internet".

[23] Recital 20.a, e-Privacy Regulation 2021 Proposal: "Where available and technically feasible, an end user may therefore grant, through software settings, consent to a specific provider for the use of processing and storage capabilities of terminal equipment for one or multiple specific purposes across one or more specific services of that provider. For example, an end-user can give consent to the use of certain types of cookies by whitelisting one or several providers for their specified purposes. Providers of software are encouraged to include settings in their software which allows end-users, in a user friendly and transparent manner, to manage consent to the storage and access to stored data in their terminal equipment by easily setting up and amending whitelists and withdrawing consent at any moment. In light of end-user's self-determination, consent directly expressed by an end-user should always prevail over software settings. Any consent requested and given by an end-user to a service should be directly implemented, without any further delay, by the applications of the end user's terminal".

[24] *I.e.* consent to a specific provider for specific purposes across specific services of that provider.

[25] Art. 4a, e-Privacy Regulation 2021 Proposal.

[26] Art. 9, e-Privacy Regulation 2017 Proposal; The principle of limiting the validity of consent in time had already been proposed long before the Regulation Proposal. Indeed, in its opinion 2/2010, the Article 29 Working Party already stated that: "consent to be monitored should not be 'for ever' but it should be valid for a limited period of time, for example, to one year. After this period, ad network providers would need to obtain a new consent. This could be achieved if cookies had a limited lifespan after they have been placed in the user's terminal equipment (and the expiry date should not be prolonged)": Article 29 Working Party, "Opinion 2/2010 on online behavioural advertising", June 22, 2010, 00909/10/EN, WP 171, p. 16, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171en.pdf.

mission can be trusted to the authorities already in charge of ensuring compliance with the GDPR.[27] [28] As a result, national data protection authorities could see an extension of both their tasks and prerogatives, as they will be able to impose administrative fines regarding GDPR as well as e-Privacy Regulation infringements. It is noteworthy that e-Privacy fines mirror those provided for by the GDPR.[29] In this aspect, it will be meaningless to try to avoid the application of a norm in favor of the other.

3. Legislative Gaps: The Cookie Wall and the Pay Wall

A new but already fundamental question is not settled in the current e-Privacy Directive: the fate of the co-called "cookie walls" and "pay walls".

The "cookie wall" also called "tracking wall"[30] is the practice by which the user is obliged to accept cookies in order to access the website.[31] The "pay wall" on the other hand, is the configuration where the user has a choice between accepting the cookies and accessing the website free of charge and accessing the website without cookies but in exchange of the payment of a fee.

About the cookie wall, the CNIL[32] had requested websites to ensure that user's consent could be as easily given as withdrawn and to offer an equivalent alternative in case of refusal before March 31, 2021.[33] The

[27] Art. 18 *et seq.*, e-Privacy Regulation 2021 Proposal.

[28] Interestingly, one of the first financial penalties imposed by the Belgian Data Protection Authority was related to cookies. With its significant amount of 15.000 euros, it translates a clear desire on the part of the Belgian DPA to set an example and send a message of intransigence when faced with violations of the legislation on cookies. (Belgian DPA, decision 12/201917, December 2019, https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-12-2019.pdf.).

[29] Art. 23, e-Privacy Regulation 2021 Proposal; Arts. 22 and 23, e-Privacy Regulation 2017 Proposal.

[30] A cookie banner where the Internet user has no choice but to accept the cookies because there is no button to refuse them is a cookie wall. We also assimilate to cookie walls the situations in which the user is not obliged to accept cookies but is obliged to deactivate adblockers to access a website. A. Delforge, "Le placement de 'cookies' sur un site Web: la Cour de justice fait le point, l'APD commence à sanctionner", *R.D.T.I.*, 2020/1-2, p. 109.

[31] M. Moné, "Cookie walls, user consent and the future of monetisation in the media", March 8, 2021, *World Association of News Publishers Website*, https://wan-ifra.org/2021/03/cookie-walls-user-consent-and-the-future-of-monetisation-in-the-media/.

[32] French Data Protection Authority.

[33] The CNIL had initially prohibited cookie walls because this contravened, in its view, the requirement of free consent. However, the French Council of State ruled that the CNIL had exceeded its powers by doing so (French Council of State, June 19, 2020, n° 434684, https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-19-juin-2020-lignes-directrices-de-la-cnil-relatives-aux-cookies-et-autres-traceurs-de-connexion). The new CNIL guidelines, adapted according to the Council

CNIL relies on the European Data Protection Board (EDPB) guidelines[34] stating that access to a website cannot be made conditional on the acceptance of cookies, in which case consent is not free. For the consent to be free, the website provider must offer *equivalent alternatives* to the user who does not want to accept cookies.

As an (unforeseen) result, from April 1, 2021, many French websites have set up a "pay wall". They justify the price for the access to the website without cookies by the loss of advertising revenue that results from the refusal of cookies. Pay walls would then constitute the equivalent alternatives as the user can refuse the cookies but still access the website.

Unlike the cookie walls, the question is not settled as to whether pay walls are legal and whether consent obtained in this way can be considered free and therefore valid. No clear answer is given by any data protection authority[35] and jurisdiction nor by the e-Privacy Directive. Although not prohibited *per se*, the legality of this practice is for the moment subject to a case-by-case assessment.[36]

Recently, two new legislative developments at the European level address the pay wall phenomenon. First, the e-Privacy Regulation 2021

---

of State's decision, now simply states that cookie walls are "likely to infringe, in certain cases, the freedom of consent" (CNIL, "Cookies and other tracking devices: the Council of State issues its decision on the CNIL guidelines", June 29, 2020, https://www.cnil.fr/en/cookies-and-other-tracking-devices-council-state-issues-its-decision-cnil-guidelines).

[34] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, May 4, 2020, §§ 37 *et seq.*, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

[35] Although no supervisory authority has taken a clear position on the legality of the pay wall, a decision of the Bavarian data protection authority indirectly accepts its legality. The case involved a service provider who offered a software for free on a platform provided that users subscribe to a newsletter. Alternatively, the same software could be obtained on another platform, without subscribing to the newsletter but for a fee.

In fine, the authority did not sanction the service provider for the pay wall. On the contrary, the authority criticized the fact that the paid alternative was available on a different platform. Thus, if it had been on the same platform as the one offering the service for free by registering to the newsletter, the consent would have been valid.

C. Piltz, "Bavarian Data Protection Authority: Newsletter registrations in return for free product – 'freely given' under GDPR?", 29 July 2021, available at: https://www.linkedin.com/pulse/bavarian-data-protection-authority-newsletter-return-free-piltz/?trackingId=ZGznqHlDD60k98QfdFbPnA%3D%3D.

[36] CNIL, "Délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux "cookies et autres traceurs") et abrogeant la délibération n° 2019-093 du 4 juillet 2019", September 17, 2020, §§ 17-18, https://www.cnil.fr/sites/default/files/atoms/files/lignes_directrices_de_la_cnil_sur_les_cookies_et_autres_traceurs.pdf .

Proposal mentioned above refers to pay walls in its recital 20aaaa.[37] In essence, the recital states that end-users have a genuine choice if they are sufficiently informed and have the possibility to choose between consenting to cookies and an equivalent offer by the same provider that does not involve this consent but still allows to access the website.

The second legislation worth mentioning is the Directive on certain aspects concerning contracts for the supply of digital content and digital services.[38] This Directive recognizes the business model of most of the websites providers which is granting access to their website free of any monetary price but in exchange with data that they will use to generate advertising revenues.[39] Hence, in contrast to the area of data protection, it appears more acceptable to monetize access to data in the area of consumer protection. However, the Directive itself provides that in case of conflict, the provisions on personal data protection prevail over the provisions of the Directive.[40]

It appears from the above that cookie walls are prohibited because the consent required by the e-Privacy legislation, which is the same under the GDPR, cannot be considered as freely given if the access to the website is purely conditional to this consent and the end-user has no other choice but to accept the cookies in order to access the website.[41]

---

[37] E-Privacy Regulation 2021 Proposal, Recital 20aaaa: "where access is provided without direct monetary payment and is made dependent on the consent (…) such consent would normally not be considered as depriving the end-user of a genuine choice if the end-user is able to choose between services, on the basis of clear, precise and user-friendly information about the purposes of cookies and similar techniques, between an offer that includes consenting to the use of cookies for additional purposes on the one hand, and an equivalent offer by the same provider that does not involve consenting to data use for additional purposes, on the other hand. Conversely, in some cases, making access to website content dependent on consent to the use of such cookies may be considered, in the presence of a clear imbalance between the end-user and the service provider as depriving the end-user of a genuine choice. This would normally be the case for websites providing certain services, such as those provided by public authorities. Similarly, such imbalance could exist where the end-user has only few or no alternatives to the service, and thus has no real choice as to the usage of cookies for instance in case of service providers in a dominant position".

[38] Directive (EU) 2019/770 of the European Parliament and of the Council on Certain Aspects Concerning Contracts for the Supply of Digital Content and Digital Services ("DCD Directive"), May 20, 2019, *O.J.*, L.136, pp. 1-27, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0770&from=EN.

[39] Recital 24 and 37 and Arts. 3.1 al. 2 and 3.7, DCD Directive.

[40] Art. 3.7, DCD Directive.

[41] Art 7.4, GDPR. Some authors speak of a presumption of invalidity of consent when access to the service is conditional on said consent. T. Leonard, "Titre 10 - Yves, si tu exploitais tes données?", in C. de Terwangne *et al.* (dir.), *Law, Norms and Freedoms in Cyberspace / Droit, normes et libertés dans le cybermonde*, 1st ed., Brussels, Larcier, 2018, p. 675.

As far as pay walls are concerned, it seems that they could be accepted under e-Privacy law if they can be considered as an equivalent alternative to the acceptance of cookies. The question whether it is equivalent or not will in the end depend on whether the fee's amount reflects the loss incurred by the website owner in terms of advertising revenues.[42]

B. Third-Party Cookies: Raw Material for RTB

While informed consent can be given regarding cookies closely related to the visit of a current website,[43] the question is less certain regarding third-party cookies.

Third-party cookies are placed by a domain different from the domain that is visited by the user.[44] They do not belong to the owner of the site whose visit generates their creation. Indeed, the data of the user is not collected by the publisher of the website but by all the advertisers who have installed a third-party cookie on this website.[45]

Those cookies allow cross-site user tracking as well as remarketing.[46] They also make a conversion measure possible. Advertisers are able to evaluate the efficiency of an ad by counting the people that this ad effectively reached and who acted upon seeing the advertisement.[47] More data are then collected for analysis or invoicing purposes, for the benefit of the advertiser.

---

[42] Some suggest that pay walls would be the only way to obtain free consent from the Internet user because the possibility to pay would constitute the equivalent alternative if it is affordable and proportionate. As a consequence, an important imbalance between the price and the value of the access to the website without cookies would therefore render the consent void. See A. DELFORGE, "Paying with Personal Data: Between Consumer and Data Protection Law", in J. HERVEG (ed.), *Deep Diving into Data Protection*, 1st ed., Brussels, Larcier, 2021, p. 59.

[43] Regarding this question, we refer to previous in-depth studies led by L. DUBOIS, F. GAULLIER, "Publicité ciblée en ligne, protection des données à caractère personnel et ePrivacy: un ménage à trois délicat", *Légicom*, n° 59, 2017/2, p. 76, https://www.cairn.info/revue-legicom-2017-2-page-69.html.

[44] Belgian DPA, Decision 12/2019, December 17, 2019, p. 31, https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-12-2019.pdf.

[45] IAB France and SNCD, "Ciblage publicitaire et respect de l'internaute", 2009, p. 16, https://www.iabfrance.com/sites/www.iabfrance.com/files/atoms/files/iab-le-ciblage-a5.pdf.

[46] Remarketing is displaying an ad for a good that the user has searched in the past but did not complete the purchase process of or has put the good in the cart but has not ordered. S. DUTTON, "Digging into the Privacy Sandbox", April 8, 2020, https://web.dev/digging-into-the-privacy-sandbox/#remarketing.

[47] *Ibid.*

As a result, the third-party advertiser and its activities are potentially unrelated to the owner of the site that the user is visiting. This makes it impossible for the user to understand where these cookies come from and for what purpose the data collected will be used. Informed consent about the identity of the data controller and the purposes of the processing can consequently be questioned.

The concerns raised by third-party cookies no longer go unnoticed and many initiatives are being launched to address the issues.

The investigators of this movement are the web browsers Mozilla Firefox and Apple Safari.[48] At the beginning of 2021, Google followed this movement by launching its "Privacy sandbox",[49] which consists of different initiatives to get rid of third-party cookies.[50] Initially announced for 2021, Google recently declared that the deployment of the Floc program which is part of the Privacy Sandbox initiative would not take place before 2023, as the Californian giant realized that it needed more time to complete this project.[51]

To this day, two major solutions are being explored in the AdTech[52] world to replace third-party cookies, namely "FloC" and first-party cookies.

---

[48] N. STATT, "Apple updates Safari's anti-tracking tech with full third-party cookie blocking", March 24, 2020, https://www.theverge.com/2020/3/24/21192830/apple-safari-intelligent-tracking-privacy-full-third-party-cookie-blocking; M. WOOD, "Today's Firefox Blocks Third-Party Tracking Cookies and Cryptomining by Default", September 3, 2019, https://blog.mozilla.org/en/products/firefox/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/; T. COËFFÉ, "Firefox va bloquer le canvas fingerprinting, une méthode de tracking sans cookie", November 2, 2017, https://www.blogdumoderateur.com/firefox-canvas-fingerprinting/.

[49] J. SCHUH, "Building a more private web: A path towards making third party cookies obsolete", January 14, 2020, https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html; See also J. SCHUH, "Privacy Sandbox in 2021: Testing a more private web", January 25, 2021, https://blog.chromium.org/2021/01/privacy-sandbox-in-2021.html.

[50] "Privacy Sandbox's mission is to create a thriving web ecosystem that is respectful of users and private by default": S. DUTTON, "Digging into the Privacy Sandbox", *op. cit*. Faced with the reluctance of the rest of the digital world following this announcement, Google confirmed in March 2021 that it would not develop an alternative technology to replace third-party cookies and that its ambition is to abandon third-party cookies on its Chrome browser by 2022. See A. SCHIFF, "Google's Message To The Ad Industry: We Won't Build Our Own Third-Party Cookie Alternatives (And We Don't Want You To Either)", March 3, 2021, https://www.adexchanger.com/online-advertising/googles-message-to-the-ad-industry-we-wont-build-our-own-third-party-cookie-alternatives-and-we-dont-want-you-to-either/; See also Google's website at: https://www.chromium.org/Home/chromium-privacy/privacy-sandbox.

[51] V. GOEL, "An updated timeline for Privacy Sandbox milestones", June 24, 2021, https://blog.google/products/chrome/updated-timeline-privacy-sandbox-milestones/.

[52] For ADvertising TECHnologies.

It is essential that it does not mark the birth of new tracking devices with the same flaws as third-party cookies. This is what we attempt to examine below.

C. Federated Learning of Cohorts ("FLoC"): The Google Alternative

Federated learning of cohorts (or FLoC) is a cookie-less protocol proposed by Google within its Privacy Sandbox program. Among the privacy-preserving APIs developed by Google, FLoC is a serious candidate to replace third-party cookies and therefore deserves all our attention.

The functioning of FLoC is based on an algorithm that runs locally on the user's device. The algorithm has access to its browsing history. However, those data never leave the user's device. Instead, the algorithm attaches the user to a cohort.[53]

The cohort consists of a group of individuals who are linked by common interests deduced from their online behavior. For example, there could be the cohort of people interested in kitchen appliances, people interested in vegetarian recipes, etc.

Only the aggregated output obtained by the algorithm will be revealed to advertisers, *i.e.* a cohort-ID. Advertisers will no longer be able to individualize each user but only decide to target one cohort rather than another.[54] In short, FloC allows the targeting of a group of people who have comparable browsing behavior.

Of course, FLoC eliminates some risks of data abuse that could be encountered with third-party cookies by the simple fact that there is no sharing or selling of users' personal data but only a disclosure of a cohort ID. However, this does not mean that all privacy concerns will disappear.

Google has made FLoC public so that it could be tested. However, the tests are only happening in non-EU countries such as the US and India. Google is not planning to conduct trials in EU countries for now, admitting that FloC could be problematic in the EU given the GDPR requirements.[55] Google refers to the involvement of the different actors engaged in the functioning of FLoC, that would not allow to link them with

[53] In reality, the algorithm will not only assign people to a cohort but will also generate these cohorts at the same time (S. DUTTON, "Digging into the Privacy Sandbox", *op. cit.*).

[54] "Google met fin aux cookies tiers dans Chrome", June 16, 2021, https://www.cookiebot.com/fr/cookies-tiers-google/.

[55] This has been confirmed by Google's engineer Michael KLEBER participating to a meeting for the Improving Web Advertising Business Group (IWABG): N. LOMAS, "Google isn't testing FLoCs in Europe yet", March 24, 2021, https://techcrunch.com/2021/03/24/

certainty to the roles defined by the GDPR ("Who is the Controller or Processor? Is there joint controllership?").[56] However, this is only one of the many problems FloC raises in terms of privacy.

First of all, even if the data is not pulled out of the user's device, there is no doubt that the operation of assigning the user to the cohort consists of a processing of personal data in the meaning of the GDPR. Since this processing can be qualified as a profiling for advertising purposes, it can only be legal if the consent of the user is obtained first.[57] This kind of brewing of data realized without the user's prior and valid approval given by a positive action (in contrast with an opt-out system) raises the same question as third-party cookies.

In the same way that it must be possible for the user to easily object to this processing, "a site should also be able to declare that it does not want to be included in the user's list of sites for cohort calculation. This can be accomplished via a new interest-cohort permissions policy".[58]

Secondly, even if the data does not leave the user's device, "Google retains access to both the raw user data stored in the browser's cache and the history of the cohorts a user belongs to. FLoC thus indeed seems to protect individuals' privacy, though not so much from Google".[59]

Thirdly, the cohorts are generated by an unsupervised Machine Learning process. There is therefore no control over which data is taken into account or how people are grouped into cohorts. Indeed, the user's navigation can reveal information about health, sexual orientation, political or religious beliefs. As a result, the key characteristics defining which cohort matches a particular user could consist in sensitive data. Then, if advertisers target their ads according to the cohort, it can end up with discriminatory advertising.[60]

Google has proposed to systematically verify that the cohort does not reveal or is not based on sensitive information.[61] If the cohort turns out

google-isnt-testing-flocs-in-europe-yet/; A. SCHIFF, "Google Will Not Run FLoC Origin Tests In Europe Due To GDPR Concerns (At Least For Now)", March 23, 2021, https://www.adexchanger.com/platforms/google-will-not-run-floc-origin-tests-in-europe-due-to-gdpr-concerns/.

[56] C. LYDEN, "Google's current FLoC tests aren't GDPR compliant", March 23, 2021, https://searchengineland.com/googles-current-floc-tests-arent-gdpr-compliant-347168.

[57] Art. 22, GDPR; A. SCHIFF, "Google Will Not Run FLoC Origin Tests in Europe Due to GDPR Concerns (At Least For Now)", *op. cit.*

[58] See https://github.com/WICG/floc.

[59] D. DECRAENE, "Google's black Sandbox", April 27, 2021, https://www.law.kuleuven.be/citip/blog/googles-black-sandbox/.

[60] For example, a dating site for homosexuals in the browsing history resulting in the attribution of the cohort ID "people with homosexual romantic preferences".

[61] See https://github.com/WICG/floc#excluding-sensitive-categories.

to be too closely related to special categories of data, the calculation must be reconducted after the parameters of the algorithms are changed to ignore those data.[62] It implies an enormous work on the part of Google which must reconfigure its AI tool. If implemented, this safeguard must be inherent to the use of FloC and not depend on the goodwill of each publisher.[63]

Fourthly, the aim of the cohort is to drown the individual in the mass of people with whom he/she/they share(s) that cohort. The cohort ID is not a unique identifier as such. However, as it is possible to aggregate data from a user's browser to attribute him/her/them a unique identifier on this basis (typically the fingerprinting process where the identifier allows to follow the user everywhere)[64], the cohort ID is a non-negligible piece of information. What is certain is that the verification that the cohorts contain enough individuals to make them unidentifiable is an essential safeguard.[65] In theory, the number of cohorts is only limited by the technological possibilities of Google which, as we all know, are rather large. The more cohorts there are, the more those cohorts are based on precise characteristics of the users' online behavior and therefore the more identifiable people are. It must then be envisaged setting up a central supervisor who will automatically count the number of cohort members and, if this number appears insufficient, bring several cohorts together.

It is planned that the cohort will be recalculated "on a weekly basis, each time using data from the previous week's browsing. This makes FLoC cohorts less useful as long-term identifiers, but it also makes them more potent measures of how users behave over time".[66]

Finally, one can wonder if FloC is not a short-term solution that would not hold the road in the long term, partly because of its current flaws but also because of the increasing requirements of data protection regulations.[67] Furthermore, to be able to replace cookies, FloC must be imple-

[62] B. Cyphers, "Google's FLoC Is a Terrible Idea", March 3, 2021, https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea.

[63] D. Bohn, "Privacy and ads in Chrome are about to become floccing complicated", March 30, 2021, https://www.theverge.com/2021/3/30/22358287/privacy-ads-google-chrome-floc-cookies-cookiepocalypse-finger-printing.

[64] CNIL, "Publicité ciblée en ligne: quels enjeux pour des données personnelles?", January 14, 2020, https://www.cnil.fr/fr/publicite-ciblee-en-ligne-quels-enjeux-pour-la-protection-des-donnees-personnelles.

[65] B. Cyphers, "Google's FLoC Is a Terrible Idea", *op. cit*.

[66] *Ibid.*

[67] C. Charman, "What Google's rejection of individual-level ad IDs means for marketers", March 8, 2021, https://www.warc.com/newsandopinion/opinion/what-googles-rejection-of-individual-level-ad-ids-means-for-marketers/4105.

mented by as many people as possible in the digital advertising sector. However, FloC acceptance seems to be already compromised as multiple actors do not plan to implement it.[68]

In light of all the above, advertisers and publishers may turn to the second replacement option: first-party cookies.

D. First-Party Cookies: A Better Alternative?

First-party data is information that companies collect themselves from their customers or people who use their own digital supports. This collection can be done by tracking tools, newsletter subscriptions, contests or surveys, loyalty, or rewards programs or even by an online brand community.[69] It is up to companies to be inventive in order to gather and leverage as much data as possible about their own audience.[70]

This type of data can be used for targeted advertising by the owner-company, or by another advertiser just as well as third-party cookies.

There are many advantages of using first-party data. First, the website's owner relies on the data it collects itself. This means that it does not depend on a third party to provide the data. It is also the opportunity for publishers and advertisers to distance themselves from the omnipotent market players.[71]

Secondly, the data comes directly from the user and is therefore more truthful, whereas third-party data may lose its accuracy through consecutive operations. It must be kept in mind that the collection of first-party data also requires the prior consent of the user when the data is actually end-users 'terminal equipment information (e-Privacy and GDPR requirement).[72] However, the fact that the data is collected directly from

[68] On the one hand FLoC is a Google API so it will necessarily work when people use Chrome. However, other browsers explicitly refused to use FLoC (Firefox, Vivaldi, Brave, and Edge) and rejected any cohort-based model: D. Decraene, "Google's black Sandbox", *op. cit.*; The same happened for some websites (edited on Wordpress for example: M. Vanroelen, "Traçage publicitaire: WordPress pourrait mettre à mal les plans de Google", April 21, 2021, https://geeko.lesoir.be/2021/04/21/tracage-publicitaire-wordpress-pourrait-mettre-a-mal-les-plans-de-google/). Moreover, the American NGO Electronic Frontier Foundation strongly opposes the Federated Learning of Cohorts system: B. Cyphers, "Google's FLoC Is a Terrible Idea", *op. cit.*

[69] N. Patel, "How to Use First-Party Data for Ad Personalization", https://neilpatel.com/blog/first-party-data/.

[70] *Ibid.*

[71] C. Charman, "What Google's rejection of individual-level ad IDs means for marketers", *op. cit.*

[72] N. Patel, "How to Use First-Party Data for Ad Personalization", *op. cit.*

the user facilitates transparency and the obtainment of consent. Indeed, the website owner collects data directly from the data subject and on this occasion can provide the data subject with all the required information.[73]

In the end, the use of first-party data for online advertising purposes will be based on information that the individual has chosen to communicate to the website. At first sight, first-party data seem way more privacy-friendly than third-party cookies and FloC.[74]

Still the question remains of the free nature of the consent collected if the consent is conditional to the access to the service (see above).

Moreover, what if some actors aggregate this data to link first-party cookies from different websites in order to link information obtained on one platform with information about the same user on another? Isn't this ultimately creating cross-site targeting that can surprise users? Former third-party intermediaries are currently developing identity solutions that aim to pool the data of each website owner to identify users. Apart from the fact that third-party cookies are replaced with first-party cookies, the intermediary would *in fine* allow to identify the same user on different websites, which is the definition of cross-site tracking.

E. Competition Issues

Aside from privacy concerns, the disappearance of third-party cookies also raises serious competition issues.

On one hand, were Google to impose its FloC solution to the AdTech industry, it would "replace an open-source and interpretable cookie tech with a proprietary one".[75] Google would become more inevitable for websites wishing to participate in the online advertising game which could "threaten the foundation of the open web".[76] Besides, the obscurity surrounding FloC could allow Google to twist its APIs to its own advantage.[77]

[73] Art. 13, GDPR.

[74] However, the website owner must have the skills and resources to manage the first-party data that it is able to gather.

[75] S. AGARWAL, "Google has an ingenious plan to kill cookies—but there's one big drawback", February 19, 2021, https://www.digitaltrends.com/features/google-cookies-alternative-chrome-privacy-sandbox-floc/.

[76] *Ibid.*

[77] D. DECRAENE, "Google's black Sandbox", *op. cit.*

Therefore, Google's initiative is already under investigation by the European Commission[78] and the UK's competition controller.[79]

On the other hand, competition concerns also arise in relation with Google regarding the first-party data solution. Google with its extended ecosystem can collect data directly from its billion users, from its search, e-mail, video, cloud services and Android mobile applications.[80] Other actors are not able to collect comparable quantities of data, allowing an anticompetitive advantage to Google regarding first-party cookies.[81]

In the end, both options generate a risk of entrenching already existing market power.

II. Real Time Bidding: A GDPR-Compliant Mechanism?

Real Time Bidding (RTB) refers to a widespread online mechanism that defines which advertisements will be displayed when a user visits a web page.

It all starts with an Internet user consulting a web page. During this consultation, data are collected (typically through the action of cookies). The data are sent to intermediaries who make a call for tenders. This

[78] Competition Policy International (CPI), "EU's Vestager Says Google's Planned Removal Of Third-Party Cookies Is An Antitrust Concern", April 25, 2021, https://www.competitionpolicyinternational.com/eus-vestager-says-googles-planned-removal-of-third-party-cookies-is-an-antitrust-concern/: Margrethe VESTAGER, the EU's competition chief, answered on behalf of the Commission: "The Commission is currently investigating the way data concerning users is gathered, processed and monetized by Google. The investigation, under the competition rules, covers the use of data and practices in the provision of 'ad tech' services, in which Google acts as intermediary between advertisers and online publishers. Google's proposals to deprecate third-party cookies are within the scope. The preliminary investigation is ongoing, and it is too early to report any findings".

[79] Competition and Markets Authority (CMA), "Final report", July 1, 2020, https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf; CMA, "CMA to investigate Google's 'Privacy Sandbox' browser changes", *Press Release*, January 8, 2021, https://www.gov.uk/government/news/cma-to-investigate-google-s-privacy-sandbox-browser-changes.

[80] Answer given by Executive Vice-President VESTAGER on behalf of the European Commission, April 23, 2021, E-000274/2021, https://www.europarl.europa.eu/doceo/document/E-9-2021-000274-ASW_EN.pdf.

[81] S. AGARWAL, "Google has an ingenious plan to kill cookies—but there's one big drawback", *op. cit.*

consists of a presentation of the users' profiles[82] based on the information collected about them.

Based on this profile, advertisers will attribute a value to the data subject while taking into account their target audience. Based on this analysis, they will bid more or less to attract the user's attention. The advertiser who proposes the highest price wins the ad spot.[83] Its advertisement is then displayed on the website and seen by the Internet user. There is no doubt that nowadays, "advertising is predominately allocated automatically through programmatic methods, of which real-time bidding is the prime system".[84]

RTB relies on data processing in the sense of the GDPR. However, this complicated, fast, obscure process involving a multitude of actors is difficult to reconcile with the data protection standard of the European Union. The Belgian Data Protection Authority has tackled the issue following a complaint.[85] Although the Belgian DPA has not yet ruled the case, its

[82] For a study about the effectiveness of this profiling, see N. Neumann, C. E. Tucker, T. Whitfield, "Frontiers: How Effective Is Third-Party Consumer Profiling? Evidence from Field Studies", 2019, *Marketing Science*, 38/6, pp. 918-926, https://doi.org/10.1287/mksc.2019.1188.

[83] EDRi, "Real Time Bidding: The auction for your attention", July 4, 2019, https://edri.org/our-work/real-time-bidding-the-auction-for-your-attention/.

[84] M. Veale, F. Zuiderveen Borgesius, "Adtech and Real-Time Bidding under European Data Protection Law", *op. cit.*, pp. 8-9.

[85] A complaint form, identifying grievances addressed to the RTB system based on the Ryan Report, is available at https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiLvdf-j8jsAhUKhRoKHVzwAWoQFjAAegQIBBAC&url=http%3A%2F%2Fwww.liguedh.be%2Fwp-content%2Fuploads%2F2019%2F06%2Fformulaire-dintroduction-dune-requ%25C3%25AAte.docx&usg=AOvVaw1ISD3dFWuDXkQieEcHWAqm.

From 2018 to 2019, no less than 14 human rights organizations filed complaints before the data protection authorities of various EU Member States regarding online behavioral advertising mechanisms. These complaints were initially filed before the Irish and UK data protection authorities and were subsequently filed in Poland, Spain, the Netherlands, Belgium, etc. They are all based on a report written by Johnny Ryan who took the initiative of the first actions. The "Ryan report" specifically targets OpenRTB and "Authorized Buyers" which is Google's proprietary RTB system (formerly called "DoubleClick Ad Exchange") and points out the different problems raised by online advertising auctions. (The Ryan Report can be found at: https://brave.com/wp-content/uploads/2018/09/Behavioural-advertising-and-personal-data.pdf). In reaction, the Irish data protection authority has officially opened an investigation (https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-opens-statutory-inquiry-google-ireland-limited) and ICO also issued a report (ICO, Update report into AdTech and real time bidding, June 20, 2019, https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf) but failed to take any action against RTB (J. Ryan, "The ICO's failure to act on RTB, the largest data breach ever recorded in the UK", January 17, 2020, https://brave.com/ico-faces-action/).

inspection department has already issued a report which identifies several compliance issues which are briefly overviewed bellow.[86]

A. Consent

According to the Article 29 Working Party, there is only one legal basis for each processing of personal data.[87] In our opinion, consent is the only legitimate ground under Article 6 GDPR that is able to justify the RTB process.

The strict interpretation of the notion of "necessity" does not allow to consider that the processing carried out by RTB actors is necessary for the performance of a contract. Any offer of service or good can have a financial counterpart so that the processing of data to finance the activity is not necessary.[88]

In Belgium, the complaint was brought before the DPA against IAB Europe by Johnny Ryan, Pierre Dewitte, Jeff Ausloos, Bruno Bidon, the NGO Panoptykon, the NGO Bits of Freedom and La Ligue des Droits de l'Homme (The League of Human Rights) (Belgian DPA, decision 01/2021, January 8, 2021, https://www.autoriteprotectiondonnees.be/publications/decision-interlocutoire-n-01-2021.pdf).

The report of the inspection committee, based on the Ryan Report has already identified problems raised by the RTB system supported by IAB Europe. As for the substance, the authority did not really take a decision. Indeed, this case made a detour to the Market Court because of a disagreement concerning the language of the procedure (Belgian Market Court, Brussel, (19th), decision 2021/AR/74, February 17, 2021, https://autoriteprotectiondonnees.be/publications/arret-du-17-fevrier-2021-de-la-cour-des-marches-ar-74-disponible-en-neerlandais.pdf). However, the issue ended with an agreement between the parties. (Belgian DPA, decision 26/2021, February 23, 2021, https://autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-26-2021.pdf). On June 11, 2021, the litigation chamber heard the parties on the merits in the case called "Ausloos et al. versus IAB Europe". The discussions were about the existence of a processing of personal data by the implementation of the Transparency & Consent Framework developed by IAB Europe (Belgian DPA Newsletter, July 2021, n° 1).

[86] P. Laloux, "La publicité en temps réel sur le Web enfreint la vie privée", October 19, 2020, https://plus.lesoir.be/332527/article/2020-10-19/la-publicite-en-temps-reel-sur-le-web-enfreint-la-vie-privee; "Plaintes contre la publicité digitale et les ventes de données personnelles aux enchères", December 13, 2020, https://www.larevuedudigital.com/plaintes-contre-les-dispositifs-de-vente-de-donnees-personnelles-par-encheres-en-publicite-digitale/; M. Jaillet, "RTB et publicité programmatique – Le framework de l'IAB viole-t-il le RGPD?", November 3, 2020, https://www.axeptio.eu/post/rtb-et-publicite-programmatique-le-framework-de-liab-viole-t-il-le-rgpd.

[87] Article 29 Working Party, "Guidelines on consent under regulation 2016/679", November 28, 2017, WP 259, rev.01, p. 22., https://ec.europa.eu/newsroom/article 29/items/623051/en.

[88] T. Léonard, "Titre 10 – Yves, si tu exploitais tes données?", *op. cit.*, pp. 663, 677 *et seq.*

At this point, we also recall that an individual's consent to enter into a contract cannot be used as consent to process that individual's data.[89]

The e-Privacy 2021 Proposal accepts the processing of cookies without the consent of the user when it is strictly necessary for providing a service specifically requested by that user.[90] In order for a contract to exist, the user must be aware of it and indicate his willingness to enter into the contract. The person surfing on the Internet does not adhere to a contract whose object is the use of their data for advertising purposes. In RTB, the Internet user just wants to have access to the website.

As for the pursuit of a legitimate interest, it can legitimate the processing only if such processing is necessary to achieve this legitimate interest and the fundamental rights and freedoms of the data subject do not take precedence. However, the mass of data processed during RTB and the lack of sufficient security measures make it difficult to fulfil these conditions even if the provider of the web page has a legitimate interest in using RTB (advertising revenues).

In conclusion, consent is the only basis of Article 6 GDPR that could establish the legality of the processing, following the e-Privacy Directive requirements, the EDPB opinion[91] and the Inspection Service of the

[89] As stated by Y. POULLET, T. LEONARD, the consent referred to in the GDPR is a unilateral act that provides the data controller with a basis for handling the data. Consent does not create a contract between the data controller and the data subject. T. LEONARD, "Titre 10 – Yves, si tu exploitais tes données?", *op. cit.*, p. 667; Y. POULLET, "Consentement et RGPD: des zones d'ombre!", *D.C.C.R.*, 2019/1-2, n° 122-123, Larcier, pp. 11-13.

As evidence of this, the GDPR requires the data controller to collect the consent for the processing separately from the consent to the contract (for example, the acceptance of the Terms and Conditions shall be distinct from the consent to the use of personal data), Art. 7.2., GDPR.

There is, however, a hypothesis where these two consents merge, namely when the contract concerns the exploitation of the data. If this exploitation constitutes the very object of the contract, the consent for the contract is equivalent to the consent for the processing of the data (but at the same time the conclusion of the contract allows the data controller to invoke the necessity for the performance of the contract as a legitimate basis of the processing). In RTB, the Internet user just wants to have access to the website. There is no question of "selling" their data.

[90] Art. 8, 1. c), e-Privacy Regulation 2021 Proposal.

[91] EDPB, Guidelines 08/2020 on the targeting of social media users, September 2, 2020 (version 1.0), § 50 *et seq.* and 66 *et seq.*, https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf, and confirmed in the EDPB Guidelines 08/2020 on the targeting of social media users, April 13, 2021 (version 2.0), § 49 *et seq.* and 72 *et seq.*, https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf.

Belgian DPA.[92] Nevertheless, it is not certain that RTB can fulfil the condition for such a consent to be valid in the meaning of GDPR.

1. Informed Consent and Transparency

Consent means "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he/she/them, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him/her/them".[93]

Article 13 of the GDPR imposes on the data controller a duty to provide information to the data subject.[94] It includes the identification of the controller, the purposes of the processing and the recipients of the data. The GDPR warns that the "proliferation of actors and the technological complexity make it hard for data subjects to understand *by whom* data is processed".[95] RTB is typically a processing of data that involves a multitude of actors playing various roles making the process very difficult to understand for Internet users, who do not know who acts as controller or processor.[96]

Data must be processed in a transparent manner. First, this means that the data controller must give the data subject information on the

[92] Irish Council for Liberties, "Data Protection Authority investigation finds that the IAB Transparency and Consent Framework infringes the GDPR", https://www.iccl.ie/digital-data/apd-iab-findings/.

In their paper, A. Custers and J.-F. Henrotte go even further when they ask whether a legal obligation can be a basis for the use of cookies. In this case, the question arose as to whether the data processing constituted by the use of cookies could be necessary to comply with a legal obligation. According to data protection law, the data controller has the obligation to take adequate technical and organizational measures to ensure the protection of the data against accidental or unauthorized destruction, loss, alteration, access, and any other unauthorized processing. However, this issue arose in relation with Facebook's "Datr" cookie. Indeed, Facebook argued that this cookie was used to secure access to its domains in order to protect its registered users. In the end, this circular reasoning was rejected by the judge. The legal obligation to take measures to secure the data cannot therefore be a legal obligation within the meaning of Article 6 of the GDPR legitimizing the processing of data which would, in the absence of this obligation, have no other legal basis to rely on. See A. Custers, J.-F. Henrotte, "Le cookie 'Datr' de Facebook: préservation de la sécurité des utilisateurs ou atteinte massive à la vie privée des internautes?", *J.L.M.B.*, 2017/26, p. 1252.

[93] Art. 4, 11°, GDPR.

[94] IAB Europe, "The EU's proposed new cookie rules: digital advertising, European media, and consumer access to online news, other content and services", December 20, 2018, https://brave.com/wp-content/uploads/2019/02/1b-IAB-2017-paper.pdf.

[95] Recital 58, GDPR.

[96] L. Dubois, F. Gaullier, "Publicité ciblée en ligne, protection des données à caractère personnel et ePrivacy: un ménage à trois délicat", *op. cit.*, pp. 75-76 and 89-91.

processing,[97] but it also means that the processing in itself must be transparent and easily understandable for the data subject. On the contrary, RTB is a black box where data is exposed and shared in an opaque system. In addition, Recital 58 clearly states that information is fundamental when it comes to online advertising.[98]

Therefore, the website owner has the obligation to inform the visitor of the identity of the recipients of the data. Yet, "with RTB it is often impossible for the website publisher to predict who will win an auction. Therefore, the publisher does not know in advance which companies (such as advertising networks) will show ads on the site. Neither does the publisher know which companies will collect data via the site".[99] [100]

Moreover, the whole RTB process takes less than a second to be completed. It takes place in the time necessary for the web page for which the user has entered a request in their browser to be displayed. It is hardly conceivable that in such a short time users have the opportunity to give real-time consent over what is done with their data.[101]

2. Explicit Consent

Data collected thanks to third-party cookies (or their successors) may, alone or in combination with others, belong to sensitive categories of data. The processing of that kind of data is prohibited unless it can rely on an exception listed in Article 9 of the GDPR.[102] The only exception that RTB can possibly rely on is the *explicit* consent of the data subject. This consent is never required in practice.

---

[97] Art. 13, GDPR.

[98] Recital 58, GDPR.

[99] M. Veale, F. Zuiderveen Borgesius, "Adtech and Real-Time Bidding under European Data Protection Law", *op. cit.*, p. 32. In theory, it is accepted to indicate the "categories of recipients" of data. However, if it is not possible to limit the information to specific categories of recipients, this information is superficial, purely hypothetical and lacks the objective of informing the data subjects sought by the GDPR.

[100] In their paper, L. Dubois and F. Gaullier briefly envisage a mechanism of standardized information spaces adapting automatically to display the identity of the data recipient in real time together with the awarding of the auction. However, this does not seem, in practice, a feasible and realistic solution. L. Dubois, F. Gaullier, "Publicité ciblée en ligne, protection des données à caractère personnel et ePrivacy: un ménage à trois délicat", *op. cit.,* p. 77.

[101] International Working Group on Data Protection in Technology, "Working Paper on the Risks emerging from the Tracking and Targeting Ecosystem in the Digital Advertising Market", *Written procedure prior the 67th (virtual) meeting on April 24, 2021*, https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2021/2021-IWGDPT-Working_Paper_tracking_eco_system.pdf.

[102] Art. 9, GDPR.

Besides, the cornerstone of RTB is the profiling of Internet users.[103] The principle of RTB is that advertisers will compete with each other and place a bid according to the value that the target represents for them. This value depends on the proximity between the profile of the user and the audience that the advertiser wishes to reach. Profiling is subject to enhanced requirements provided for in Article 22 of the GDPR. According to this article, profiling can only take place if the data subject has given their *explicit* consent.[104]

To be valid, the consent requires a prior, unambiguous, and affirmative action by data subjects indicating acceptance to cookies.[105]

3. Proof of consent

As data are moved between different actors, it can be complicated to ensure that the processing is actually based on a consent originally given by the data subject.

To solve this problem, an additional actor has been introduced into the RTB process: the Consent Management Platform (CMP) whose task is to centralize the consent of users. CMP allows "a large number of third parties [to] simultaneously seek consent from a data subject in one action. The attempt to get simultaneous consent can and does end up with consent sought for hundreds of vendors at once. (…) The publisher accepting global consent would have no proof that consent was ever obtained. The publisher would also be liable as part of a joint controllership operation for a legal action undertaken on the basis of accepting this unverified consent signal, even were it to be theoretically possible to accept as valid".[106]

---

[103] International Working Group on Data Protection in Technology, "Working Paper on the Risks emerging from the Tracking and Targeting Ecosystem in the Digital Advertising Market", *op. cit.*

[104] Art. 22, GDPR.

[105] Article 29 Working Party, "Opinion 2/2010 on online behavioural advertising", *op. cit.*, p. 3. In the Planet 49 Case, the CJEU confirmed that a pre-checked box does not fulfil the requirement of explicit consent in the sense of the data protection legislation. See A. Jablonowska, A. Michałowicz, "Planet49: Pre-Ticked Checkboxes Are Not Sufficient to Convey User's Consent to the Storage of Cookies", 1/2020 *EDPL*, p. 140, https://doi.org/10.21552/edpl/2020/1/19: "consent – as one of available legal grounds for the processing of personal data – constitutes a qualified opt-in standard, and introduced the principles of privacy by design and privacy by default".

[106] M. Veale, F. Zuiderveen Borgesius, "Adtech and Real-Time Bidding under European Data Protection Law", *op. cit.*, pp. 25-29.

B. Qualification of Actors

The RTB mechanism is much more complex than it seems. In reality, there is not only an advertiser and a publisher but a myriad of intermediaries who make this auction easier or more efficient: the supply-side-platform centralizes the offers of publishers, the demand-side-platform places bids on behalf of the advertisers and ad-exchanges organize the auction in itself.

Furthermore, defining the roles and responsibilities of the various actors involved in RTB is a complex task.[107] This can be problematic as the definition of the roles can imply specific responsibilities and the obligation to make additional agreements. In practice, there is also a problem of consistency when an actor is given different qualifications for the provision of the same service.

C. Data Minimization

In order to permit the auction, the publishers must issue a maximum of information on the Internet users. To do this, publishers draw up their profile as precisely as possible based on personal data collected through cookies.[108] The more precise the profile, the more interesting it is for advertisers. However, collecting as much data as possible goes against the principle of data minimization.[109] Revealing the profile of each user to potential advertisers without knowing exactly who will have access to it or who will win the bid and use these data also violates this principle.[110]

D. Security

Finally, the security requirements imposed by the GDPR must be met for every processing. RTB is no exception to the rule. According to this

[107] In its guidelines on the tracking of social media users, the EDPB considers that when it comes to profiling, the advertiser and the website publishers are jointly responsible for the processing consisting of targeted advertising: EDPB, Guidelines 08/2020 (version 1) on the targeting of social media users, *op. cit.*, §§ 31 *et seq*.

[108] CJEU, case "Planet49", *op. cit.*: "(…) the collection of that data by means of cookies is a form of processing of personal data". Since cookies can be used to collect personal data and since the obscurity of the RTB phenomenon does not allow us to know, precisely, which data is collected, there is a risk that personal data is collected.

[109] Art. 5.1.c), GDPR.

[110] Given the functioning of RTB, even if advertisers do not receive the information themselves, the intermediaries who act as their processors will have access to this information to be able to evaluate the price they will offer in the auction.

principle, the data controller has the obligation to ensure that the processing of personal data only occurs if technical and organizational measures ensuring the security of the data are taken. Those measures are designed to protect data against unauthorized or unlawful access or more generally against any kind of data violation.[111] In its case law, the European Court of Justice advised to take into account, in order to determine the security level needed, the quantity of personal data, the data's sensitivity, and the risks generated by the processing.[112] If we compare RTB to those criteria, we quickly realize that RTB requires a high level of security.

In addition, studies shows that when the RTB process is happening, leakages of data can happen.[113]

III. Perspective

The disappearance of third-party cookies will significantly impact the current functioning of the open Internet, online marketing, and RTB.

It is essential to monitor the future development of the online advertising landscape to ensure that the end of third-party cookies is a real step forward in data protection and that these efforts are not undermined by mechanisms such as RTB that would continue to exist based on the third-party cookies successors.

A solution that solves most of the issues is contextual advertising. As its name suggests, it is not based on the interests and personal data of the individual but on the environment in which the ad will be displayed. In fact, advertisers choose where to display their advertisement based on the content of the website. As it does not rely at all on the individual's personal data,[114] it is future-proof against the evolutions of data protection regulations.

The end of online tracking may not be the catastrophe that frightens the AdTech industry. There is indeed scarce study on the effectiveness of ad targeting for advertisers, assuming that, given the budget spent by

---

[111] Art. 32, GDPR.

[112] CJEU, *Maximillian Schrems v. Data Protection Commissioner* (case "Schrems I"), October 6, 2015, C-362/14, ECLI:EU:C:2015:650, § 91.

[113] L. Olejnik, T. Minh-Dung, C. Castellucia, "Selling Off Privacy at Auction", *HAL*, December 6, 2013, p. 7, https://hal.inria.fr/hal-00915249/PDF/SellingOffPrivacyAtAuction.pdf.

[114] IAB Europe, "Guide to the Post Third-Party Cookie Era", February 2021, https://iabeurope.eu/knowledge-hub/iab-europe-guide-to-the-post-third-party-cookie-era-updated-in-february-2020/.

companies, it must be effective.[115] It is true that, due to the multiplicity of factors that lead to the act of buying a product, the presence of click-bots and the opacity of the RTB mechanism, concrete results are difficult to measure. Nevertheless, due to the growing ad-blindness of Internet users, it seems that click-through rates have already dropped.[116]

Nonetheless, a recent study from the publishers' side shows that the revenue drop for publishers is only about 4%[117] when the ad does not rely on cookies. This difference may be worth the privacy concerns and related investments spared by the publishers, as well as the privacy-savvy audience that would be lost.[118]

No one knows what the future holds regarding online advertising, only that the Adtech industry's resilience is strong, and that the regulation always lays one step behind it.

[115] S. DUBNER, "Does Advertising Actually Work? (Part 2: Digital)", *Freakonomics podcast*, ep. 441, November 25, 2020, https://freakonomics.com/podcast/advertising-part-2/.

[116] *Ibid.*

[117] This corresponds to an average increase of $0.00008 per advertisement based on cookies.

[118] V. MAROTTA, V. ABHISHEK, A. ACQUISTI, "Online Tracking and Publishers' Revenues: An Empirical Analysis", 2019, https://weis2017.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf.