Eliëtte Vaal, Vonne Laan, Matthias de Bruyne

The cookie has crumbled: custom audiences to the rescue?

The digital marketing industry is in reform. For the past 25 years, third-party cookie-tracking has been one of the most important tools for online targeting and retargeting. How do things stand now? Are cookies future-proof or has the cookie crumbled, with custom audiences on social media platforms coming to the rescue?

Cookies and the applicable legal framework

We all know the standard phrasing in cookie statements. But cookies and similar technologies are in essence nothing more than small bits of data that can be placed on your laptop or other device and used to recognize website visitors. They are therefore ideal for marketing purposes, where recognizing who has clicked on your ad is essential. However, using cookies means facing tough legal challenges. In the Netherlands, two legal regimes apply to the online tracking of customers: the ePrivacy and the GDPR regimes. The current ePrivacy regime is based on the ePrivacy Directive (2002/58/EC, amended by Directive 2009/136/EC), implemented in the Telecommunications Act, while the GDPR has been transposed into the General Data Protection Regulation Implementation Act. The combination of the ePrivacy and the GDPR regimes determines whether an opt-in is required or an opt-out is sufficient.

"Using cookies means facing tough legal challenges."

When targeting practices involve the use of cookies (or similar technologies such as pixels, tags, or beacons), the main rule is that prior consent is required. Under the Dutch Telecommunications Act, the use of cookies for analytic purposes also requires an opt-in, except where they have limited or no impact on the privacy of end-users (so-called 'privacy friendly' analytic cookies). Strictly functional cookies do not require consent either. This is the case if their sole purpose is to facilitate communication over an electronic communication network, or if storage of or access to the data is strictly necessary for providing the information-society service requested by the website visitor.

Thus, under the ePrivacy rules, targeting and retargeting cookies requires consent. Consent is any freely given, specific, informed, unambiguous and advance indication of the data subject's wishes. This implies a real choice as well as control when providing consent via cookie banners. The European Court of Justice has confirmed that pre-ticked boxes are not allowed (C-61/19). Furthermore, a regional court in Germany has held that misleading cookie banners that do not present consent to and refusal of cookies as equivalent options do not meet the requirements of German law. Excessive cookie banners and pop-ups would therefore appear to be inevitable. All hope is now vested in new legislation to resolve this issue. On February 10th, the Council of the European Union finally published a new proposal for an ePrivacy Regulation. It is the fourteenth in a long series of attempts by EU presidencies to find common ground following the European Commission's 2017 proposal. Ambassadors from the Council of the European Union have agreed on this latest version for a negotiating mandate, finally leading to some movement in the legislative process of the ePrivacy Regulation. The next step in the process is the trilogue, in which the Parliament, Council and Commission of the European Union will come together to hammer out the final text.

Just like the GDPR, the ePrivacy Regulation is part of the EU Digital Single Market Strategy. Its aim is to update the current, outdated ePrivacy regime by safeguarding the privacy of the end-users, the confidentiality of their communications, and the integrity of their devices. And although this proposal does not explicitly mention the option of providing consent via browser settings as was the case in the proposal by the European Commission, it does seem to give a little ground in this regard. Having regard to the prevailing consent fatigue, the recitals state: "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." Thus, consent via browser settings seems to be allowed, but only if the browser settings offer the possibility of providing granular consent as regards the parties and purposes concerned. If they do not, then cookie banners and cookie pop-ups will continue to be a necessary evil. Unless you don't use cookies. Recently, for instance, publishers such as the New York Times and the advertising platform STER announced that they have abandoned the use of third-party tracking cookies. With Google Chrome's announcement that it will phase out all support for third-party cookies over the next year, thus joining Safari and Firefox who are restricting third-party cookies in their web browsers, the end of the third-party cookie era seems nigh.

Custom audiences and the related legal framework

In the absence of third-party cookies recognizing customers on their websites, organisations are looking for alternatives to targeting customers. One such existing and popular form of online targeting is known as 'custom audiences' or 'list-based' targeting. An advertiser uploads a list of email addresses, phone numbers, cookie-IDs or other identifiers of its own customers or prospects to a platform, such as Facebook. The platform then uses a process called matching to identify customers or prospects on its own platform. This enables the advertiser to either target its own customers and prospects with a personalized campaign or exclude them to save online advertising costs.

But what is the situation in the Netherlands? How are custom audiences used here? At our request, the Data Driven Marketing Association (DDMA) carried out a survey to find out more about the use of custom audiences in the Dutch market. Most commonly, custom audiences are being used to exclude current customers from marketing campaigns and to focus solely on prospects (most likely to reduce advertisement costs). The majority of the participants in the survey also use custom audiences to create so-called lookalike audiences, a group of new customers selected by the platform based on the advertiser's common parameters for current customers. In addition, the platforms most frequently used for custom audiences (by the respondents) are Google and Facebook, followed by LinkedIn and Instagram. However, the survey showed that there is still uncertainty about the rules that apply to custom audiences. When is consent required?

Direct marketing through electronic messaging (email/SMS/personal messages on social media) requires prior consent under the ePrivacy rules. Although the exact scope of this requirement is not clear, it does not necessarily apply to custom audiences, as it seems defensible that the majority of such advertisements do not qualify as electronic messages under the Telecommunications Act. It remains to be seen whether this will change under the new ePrivacy regulation. It will depend on the exact interpretation of electronic messaging. But how are consent requirements regulated under the GDPR?

If no consent is required under ePrivacy, then, under the GDPR, there may still be a requirement to obtain consent for the processing of the personal data. This depends on whether a so-called legitimate interest can be relied upon

"The platforms most frequently used for custom audiences are Google and Facebook, followed by LinkedIn and Instagram."

or not. The conditions for a legitimate interest to apply are: (i) the existence of a legitimate interest that is to be pursued; (ii) necessity and (iii) proportionality (whether the legitimate interest is overridden by the individual's fundamental rights and freedoms. Although this may sound like a rather theoretical exercise, the European Data Protection Authorities, united in the European Data Protection Board (EDPB), recently provided two practical examples in relation to custom audiences in their draft guidelines on the targeting of social media users.

In the first example, a Bank provides the email address of a prospect to a social media platform to enable the platform to match it with its users' email addresses and thus identify and target the individual on the platform. In the second example, the Bank provides the email address of an existing customer for the same purpose. According to the EDPB, this legitimate interest may be relied upon when targeting the existing customer in this example, on condition that; (i) the customer was informed that their contact details would be used for direct marketing by the company, (ii) the advertisement relates to the services similar of those provided to the customer, and (iii) the customer was given the opportunity to object when the contact details were collected. As regards the targeting of the prospect, however, consent is required according the EDPB, as the prospect does not have the reasonable expectation that their contact details will be used for targeting on social media. Consequently, targeting prospects seems to require the consent of the individual concerned. However, it remains unclear to which extent this has been influenced by the specifics of this case. This may be clarified in the final version of the guideline.

In practice, organisations rarely collect data for the purpose of targeting customers on platforms but, rather, they use their existing customer database. The use of personal data for subsequent processing for custom audience purposes, such as sharing email address, matching, selecting targeting criteria, displaying advertisements and ad reporting, needs to be compatible with

the initial purpose of the processing. This is the principle of purpose limitation. It may be argued that the use of existing customers' email addresses to target those customers on social media and send them newsletters for marketing purposes is a purpose compatible with the collection of those email addresses. However, if personal data is collected for other purposes, such as in the course of customer service, processing for direct marketing purposes is probably not compatible and consent is required before the data can be used in the custom audience scenario.

Plan of action?

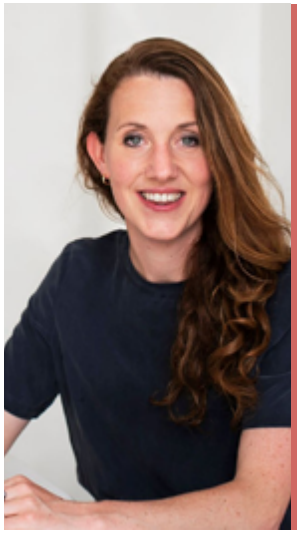
Until browsers provide the option to grant granular consent, there is no real solution to the problem of consent fatigue on the web. At this point, if you use tracking cookies, you still need to work with cookie banners or cookie pop-ups etc. Organizations wishing to investigate alternatives to tracking cookies can of course examine custom audience options. A Data Protection Impact Assessment (DPIA) is recommended to determine whether consent is required in that scenario, including with a view to the new purposes envisaged for an existing data set. Basically, a DPIA is a questionnaire that guides you through all the privacy elements that need to be considered. It provides a structured method for documenting and improving privacy compliance for a new version of a custom audience that you may want to use, for example. Regardless of the so-called purposes limitation, the chances are that you will need consent for the custom audience scenario if you target prospects rather than your existing customers. If you target existing customers, you may not need consent if you are able to substantiate your legitimate interest in the DPIA.

Businesses may therefore need to complete a lot of DPIAs. Fun times ahead!

In short:

- Under the current (e)Privacy rules, targeting and retargeting cookies require consent;
- The new version of the ePrivacy Regulation has regards to the prevailing consent fatigue. However, it is expected that cookie banners and cookie pop-ups will continue to be necessary;
- 'Custom audiences' is an alternative to target customers online. According to the EDPB, this alternative does not always require consent when targeting existing customers;
- A Data Protection Impact Assessment is recommended to determine whether consent is required, including with a view to new processing purposes envisaged for an existing data set.

About the author
Matthias de Bruyne is Senior Legal Counsel at the DMMA, the main data-driven marketing association of the Netherlands. He contributed to this article by providing input on the use of custom audiences in practice.



About the author
Eliëtte Vaal is a lawyer and partner at The Data Lawyers. Eliëtte handles cases in relation to new technologies, e-privacy, e-commerce, copyright law and freedom of expression. Eliëtte advises on compliance and assists clients in enforcement procedures initiated by the Data Protection Authority.

About the author
Vonne Laan is a lawyer and partner at The Data Lawyers. She assists Dutch and international clients with various matters in the field of privacy, data protection and cybersecurity. Furthermore, she is a frequent speaker at conferences and guest lecturer at Nyenrode Business University and the Windesheim University of Applied Sciences.