IAB Europe Ad Blocking Detection Guidance

Guidance for implementing the IAB D.E.A.L. under EU privacy laws

About IAB Europe

IAB Europe is the voice of digital business and the leading European-level industry association for the interactive advertising ecosystem. Its mission is to promote the development of this innovative sector by shaping the regulatory environment, investing in research and education, and developing and facilitating the uptake of business standards.

Contact

Matthias Matthiesen (matthiesen@iabeurope.eu)
Public Policy Manager,
IAB Europe

Executive Summary

- Ad blocker detection is not illegal, but might, under a strict interpretation of the ePrivacy Directive be regulated and require the informed consent of users.

- Depending on the technical implementation of ad blocker detection, such detection may be out of scope of the consent requirement of the ePrivacy Directive, or fall within an exemption to the consent requirement. But the legal situation is not very clear.

- Publishers who use ad blocker detection should update their privacy policy to include use of ad blocker detection scripts.

- Publishers may want to err on the side of caution and obtain consent for the use of ad blocker detection scripts to preempt and avoid any legal challenges.

- Publishers could obtain consent by slightly modifying their existing compliance mechanisms for the use of cookies as the possible new consent requirement emanates from the same law mandating consent for the use of cookies.

- Publishers could use two practical solutions to request and obtain consent for the use of ad blocker detection: a consent banner or a consent wall. Publishers could also make use of a combination of the two to complement each other.

Contents

Overview

On 7 March 2016, the IAB Tech Lab published its Publisher Ad Blocking Primer describing a range of tactics that publishers can deploy individually or in tandem in order to mitigate concerns about the impact of ad blocking.

The primer suggests that publishers follow the D.E.A.L. process, applying the tactics deemed appropriate based on the publishers' relationship with their audience, as well as other factors:

Detect ad blocking, in order to initiate the conversation.
Explain the value exchange that advertising enables.
Ask for changed behavior in order to maintain an equitable exchange.
Lift restrictions or **L**imit access in response to consumer choices.

To assist IAB members globally to make use of the D.E.A.L. process, the IAB Tech Lab developed the Ad Blocking Detection Code allowing publishers to detect the presence of an ad blocker and enabling publishers to initiate the conversation.

IAB Europe believes that publishers should be allowed to take reasonable measures to ensure that their audience understands the value exchange that advertising enables and argues EU privacy rules should not be interpreted as meaning that publishers are required to ask for permission from users to detect ad blocking in most circumstances.

Nevertheless, the legal situation under EU privacy rules, specifically the ePrivacy Directive (also known as the "Cookie Directive"), is not entirely clear and some publishers may wish to err on the side of caution and satisfy even the most extreme interpretations of the ePrivacy Directive's limitation on the access and storage of information on users' devices by obtaining the user's consent.

The below guidance describes how publishers can minimize legal exposure by implementing either a "consent banner", a "consent wall", or a combination of the two to obtain consent for the storing and accessing of information on users' devices in line with common practical interpretations of the ePrivacy Directive. In any case it is recommended that publishers update their privacy policies to reflect the use of ad blocker detection.

As the legal requirements for requesting and obtaining permission for the purpose of storing and accessing of information on users' devices vary amongst the member states of the European Union,[1] publishers may also want to seek advice from their local IAB or consult with local legal counsel to get the most accurate advice for their particular situation.

[1] *See* IAB Europe's ePrivacy Implementation Center under <www.iabeurope.eu/eucookielaws>

The Cookie Directive and Ad Blocker Detection

There are potential regulatory concerns about ad blocker detection, which stem from the ePrivacy Directive, also known as the 'Cookie Directive'. Specifically, it is Article 5(3) of the ePrivacy Directive that may apply to ad blocker detection:

> Article 5(3)
> "Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service."

The provision applies where information is stored on a user's device, or where information already stored is accessed from a user's device. Although it was originally intended to cover cookies, and similar technologies, the use of the words "any information" allows the provision's scope to be interpreted to apply to an extremely broad set of circumstances, including, for example, any processing which influences the behavior of a device, or otherwise causes it to store or give access to information on that device. Even information exposed by the device itself, such as device IDs, browser type, etc.

Moreover, for the purposes of the ePrivacy Directive it is irrelevant whether the information in question present a privacy or data protection risk. It is not limited in scope to personal data but covers any information, personal or not.

The law provides for only two, very narrowly drawn exemptions. One for storage or access that is strictly necessary for transmitting a communication over telecommunications network. Another for storage or access that is strictly necessary for an information society service explicitly requested by the user to provide the service.

The Article 29 Working Party which consists of the data protection authorities of every EU member state has opined that this means that access to information for analytics purposes is not exempted and therefore requires consent. On the other hand, the group has also opined that access to information to adapt content to the characteristics of a device is exempted and therefore does not require consent.

The Article 29 Working Party is an advisory body and its opinions are not binding – but their opinions showcase that the legal situation regarding ad blocker detection is far from clear.

An EU Law-Compliant D.E.A.L.

European publishers that want to implement the D.E.A.L. in Europe have a number of options available to them, including arguing that the requirement in the ePrivacy Directive to obtain consent for storing or accessing information on a user's device is not applicable to the detection of ad blocking, or ad blocker detection is covered by one of the provision's exemptions..

> **Option 0:** Continuing without obtaining consent. Publishers could argue that exceptions to the consent requirement of the ePrivacy Directive for other technically equivalent detection scripts for the purpose of, e.g. responsive design, also cover the use of ad blocker detection.
>
> **Option 1:** The "consent banner" – a banner positioned in a visible location at the top or bottom of a user's browser. The banner contains information about the technologies for which the publisher would like to request a user's consent and the notice that continuing to use the website will be interpreted as consent for use of those technologies (in the same way that some publishers currently obtain consent for the use of cookies). The banner would also contain a link to the publisher's privacy policy with more detailed additional information.
>
> **Option 2:** The "consent wall" – an interstitial site shown to first time visitors of a site. The interstitial site provides users with information about the technologies for which the publisher would like to request a user's permission and a consent request. A user who has agreed to the use of the technologies concerned will then be redirected accordingly.

While Option 0 is a defensible position, it does not provide the same security of either Option 1 or Option 2, which are in line with existing guidelines from EU privacy regulators for storage and access of information on a device, namely cookies, and minimize potential legal liabilities associated with detecting the use of ad blockers. These methods can also double as requesting consent for the use of cookies and in some cases only small modifications are necessary to address compliance concerns. Both methods have their advantages and disadvantages.

Privacy Policy Update

Irrespective of the choice publishers make on whether to and how to obtain consent for the use of ad blocker detection, their privacy policy should be updated to reflect that ad blocker detection is taking place and what a publisher is doing with that information.

The privacy policy should be sufficiently comprehensive and understandable so as to allow individuals to understand the potential impact on their privacy and consequences of ad blocker detection. It should include the following information:

(i) Publishers making use of ad blocker detection should provide information about their detection method and its technical implementation. The level of detail of the information provided on ad blocker detection should be in line with the remainder of the privacy policy.

(ii) Publishers should describe what they are doing with the information about the presence, or lack thereof, of an ad blocker, e.g. restriction, redirection, notification, analytics, etc.

(iii) Users need to be informed about their right to to withdraw their consent, or opt-out of ad blocker detection. If a user's consent state is stored in a cookie, publishers could simply request that users delete cookies from their browser, or facilitate deletion of the cookie specifically storing the consent-state. This could also be combined with the existing opt-out mechanism for cookies, or be offered as a separate opt-out for ad blocker detection. Where appropriate, publishers should inform the user that access to the website may be restricted where they do not agree to the use of ad blocker detection.

Example information for use in a privacy policy:

> *"Our website uses JavaScript to detect the use of ad blocking extensions for web browsers. This script is implemented in the source code of our website. The script simulates the display of an ad and confirms that it is displayed on a user's device. To do this, we do not store any information on users' devices and process no personal data. If we detect that a user deploys an ad blocker, we may interact with them on the use of ad blockers and/or adapt the content available to them. If a user no longer wants us to use ad blocker detection mechanisms, they may opt-out by clicking here. We then will store the information that the user does not want us to use ad blocker detection mechanisms in a cookie on their device. We reserve the right to restrict access to our websites if users do not agree to the use of ad blocker detection mechanisms."*

Option 0: Continue Without obtaining Consent

Publishers could continue using ad blocker detection protocols without asking permission from the user, arguing that ad blocker detection falls outside of the scope of Article 5(3) of the ePrivacy Directive, or arguing that it benefits from the exemptions of the consent requirement.

A strict interpretation of the law could mean that ad blocker detection falls within scope of the consent requirement of Article 5(3) of the ePrivacy Directive as information about the device's or browser's characteristics (capable of displaying ads, or not) are being revealed, which could potentially be interpreted as accessing information stored on the device. Likewise, it is not possible to say with certainty that ad blocker detection benefits from one of the exemptions of Article 5(3). However, it is a defensible position considering that technically equivalent detection for the purpose of responsive webdesign, or detecting available video plugins, is exempted.

Publishers who want to minimize any legal exposure should therefore consider requesting and obtaining permission from users for the use of ad blocker detection.

Option 1: Consent Banner

The first option publishers have for requesting and obtaining consent from users for ad blocker detection, without the need to outright restrict access to all users unless they have agreed to the use of detection protocols, is to make use of a layered privacy notice through the use of a 'consent banner'.

A layered privacy notice provides the user of privacy related information in two layers. First, the user is provided with information about the publisher's use of cookies and other technologies, as well as the purpose for which they are used, and a link to the publisher's privacy policy. The user should also be informed that continuing to use the site will be considered as his or her agreement to the publisher's privacy policy. The consent request can be formulated in such a way as to also cover the use of cookies, so that information about a user's consent state may be stored in a cookie.

This may be done, e.g. in a banner, which must be prominently displayed at the top or bottom of the site. As ad blocker detection is not very privacy intrusive it is not necessary to explicitly mention it in the information of the consent banner. It is however necessary to explicitly mention it in the privacy policy (*see above*).

Example:

> *"We use technologies, such as cookies, to customise content and advertising, to provide social media features and to analyse traffic to the site. By continuing to use our site you agree to our privacy policy. [OK]"*[2]

Once a user agrees to the use of cookies and other technologies as described in the privacy policy, the ad blocker detection script can be executed. Which actions exactly constitute agreement by further use are different from market to market. In principle any action can be interpreted as further use that constitutes consent, including clicking on an 'accept' button, scrolling the site, clicking on a link, clicking on an image, highlighting text, and more.

In order to make sure that consent has actually been granted before execution of the script, it should be held back from running until the consent action has been detected.

A user who is merely seeking additional information by clicking on the privacy policy link should not be considered as having agreed to the terms presented in them. However, further use of the website after having accessed the privacy policy may be construed as consent. The privacy policy should also provide information and a way to withdraw consent, but publishers may refuse access to their website to those users who do not consent or withdraw consent to their making use of ad blocker detection.

The disadvantage of a consent banner is that a publisher cannot immediately prevent a user accessing content on first visit, as the script should only be executed once the user has engaged in an affirmative action that can be construed as meaning consent. So, for example, a user who arrives at a page via a direct link, and who does not access any other content on the site, would be able to view the content as they do not engage in an affirmative action that would allow the publisher to say that consent for the use of cookies and ad blocker detection has been granted, and would-be ad blockers would not be detected. However, a consent banner allows publishers to detect ad blocking without significantly negatively impacting the user experience of users who have not installed an ad blocker.

Local market differences on the definition of 'consent'

Depending on the market, the local implementation of the ePrivacy Directive does not necessarily require withholding setting of cookies until an affirmative action has

[2] *See* IAB Europe Guidance "Five Practical Steps to help companies compy with the E-Privacy Directive under <http://www.iabeurope.eu/files/1414/3650/6858/IAB_Europe_Guidance_-_Five_Practical_Steps_to_Comply_with_EU_ePrivacy_Directive.pdf>

been detected, as consent may not be required at all, or may be construed from the fact that a user has not refused their use.[3]

In principle, an implementation of the ePrivacy Directive as described above would allow the use of an ad blocker detection script right away, but would still require informing users that a detection script is being used. In addition, users would have to be offered a right to refuse the use of a detection script after the fact. This creates complications because the real-time character of ad blocker detection makes it impossible to opt-out retrospectively, which is possible for cookies due to their persistence and the fact that they can be subsequently deleted. Therefore, when it comes to obtaining consent for ad blocker detection, where refusing consent results in an action such as restricting access to a publisher's website, only an affirmative action opt-in seems to make sense.

However, this is not a limiting factor where ad blocker detection is done for analytics purposes only, and not to restrict access. In that case, depending on the local implementation of the cookie provision, ad blocker detection could also take place immediately, provided that the necessary information and a right to opt-out is provided, i.e. by using a layered privacy notice using a consent banner as described above.

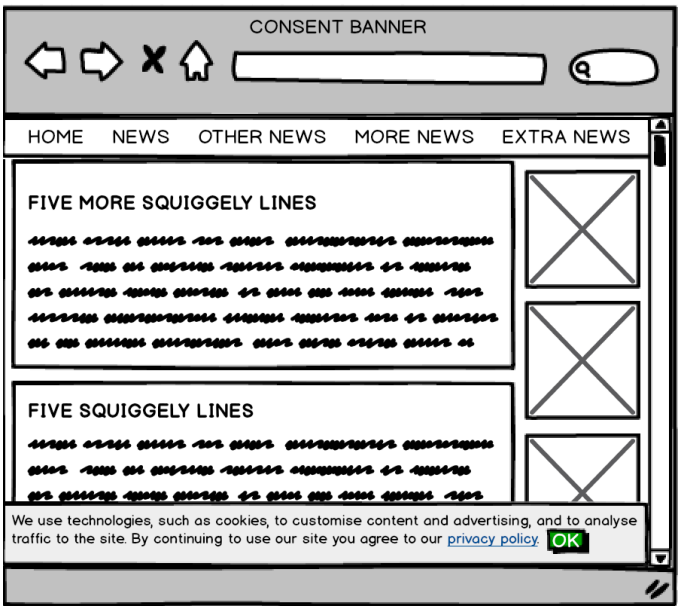

Figure 1. The user has arrived on the site and is provided with a consent banner that informs them about technologies used, provides a link to the full privacy policy and explains that continued use of the site is consent to the policy. The ad blocker detection script should not be executed at this stage.

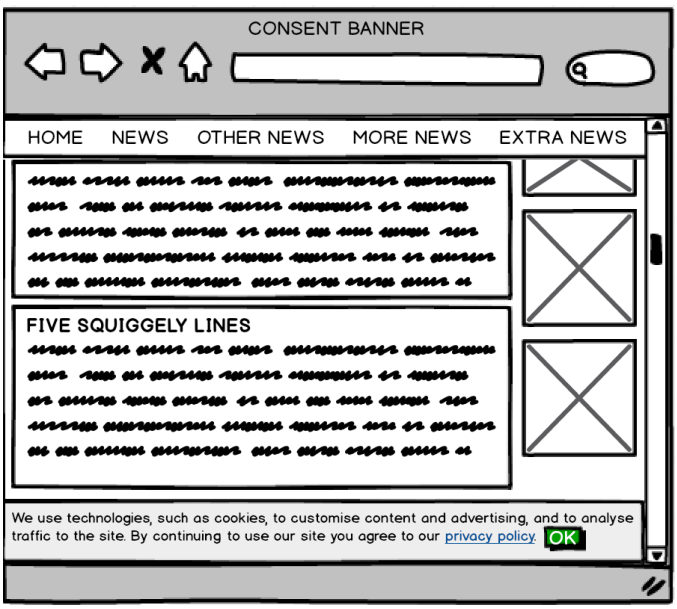

Figure 2. The user has scrolled down the site after having been informed that using the site constitutes consent to the privacy policy. At this stage, the ad blocker detection script should be executed and appropriate measures taken as a result. Cookies should be set to remember that the user has consented.

[3] *See* IAB Europe's ePrivacy Implementation Center under <http://www.iabeurope.eu/eucookielaws>

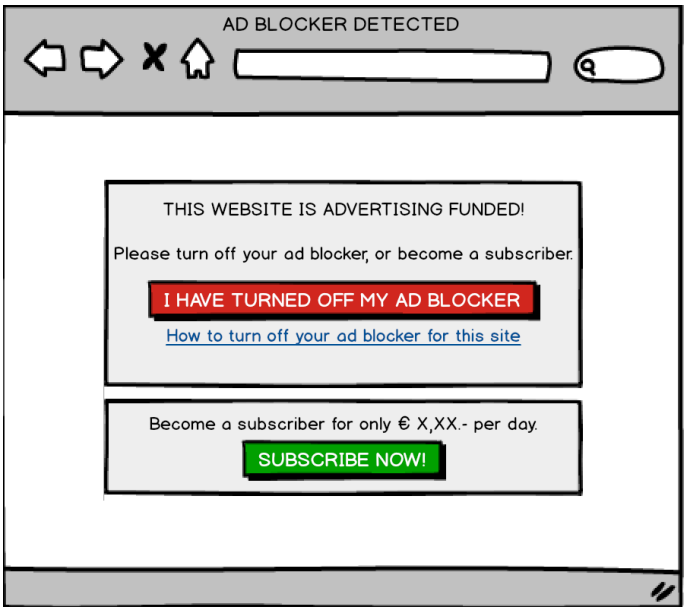

Figure 3. The ad blocker detection script detected the presence of an ad blocker and redirects the user to a website explaining the value exchange and asking them to turn off their ad blocker or subscribe.

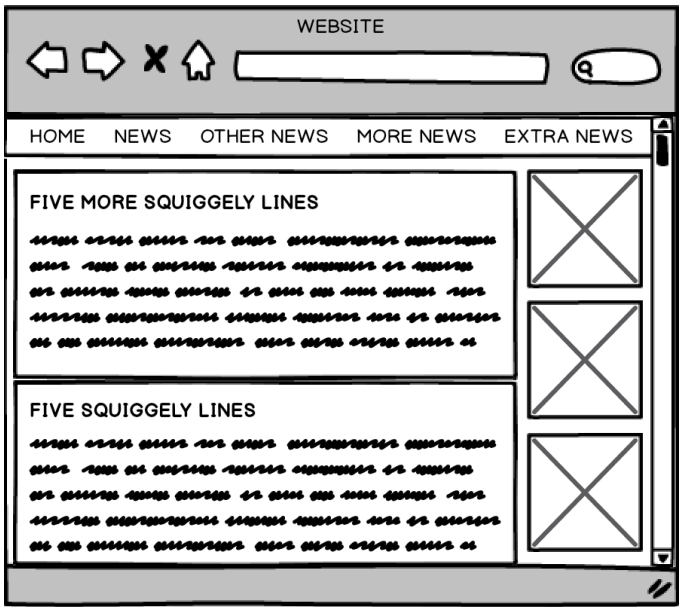

Figure 4. The user has subscribed or turned off their ad blocker or no ad blocker was detected to begin with, so the user has unrestricted access to the publisher's website (again).

Option 2: Consent Wall

The second option publishers have for requesting and obtaining consent from users for ad blocker detection is to restrict access to the publisher's website until consent for the use of detection protocols has been given.

This can be done through a 'consent wall', an interstitial page displayed to all first time visitors of a website, or users who have not previously granted consent for the use of detection protocols. The interstitial page should provide information about the use of cookies and other technologies, which would include ad blocker detection, as well as the purpose for which they are used and a link to the publisher's privacy policy containing more detailed information. As ad blocker detection is not very privacy intrusive it is not necessary to explicitly mention it in the information given in the consent wall. It is however necessary to explicitly mention it in the privacy policy. Users should also be asked to agree to their use via an 'accept' or 'agree' button.

The consent request could be formulated to also cover the use of cookies so that information about a user's consent status may be stored in a cookie to stop him or her from being served with the consent wall the next time he or she visits the site. Once a user has agreed to the use of cookies and other technologies as described in the privacy policy, the ad blocker detection script can be executed.

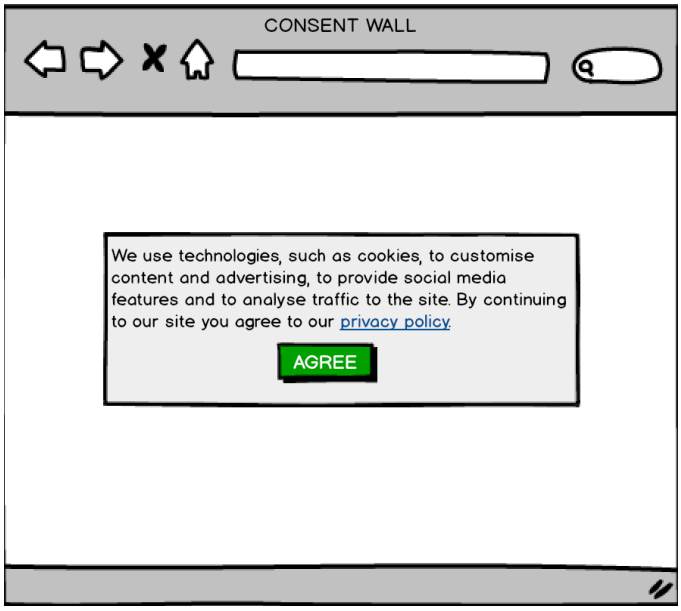

Figure 5. The user visits the publisher's site and is presented with a consent wall, informing about the use of certain technologies and providing a link to the privacy policy. The user must now agree before being allowed to access the site. Cookies should be set to remember the user's consent to these measures in order to skip this step when they visit the site next time.

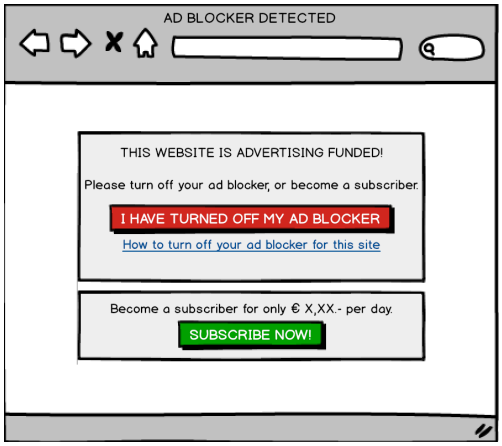

Figure 6. The user has an ad blocker installed and access to the site is restricted...

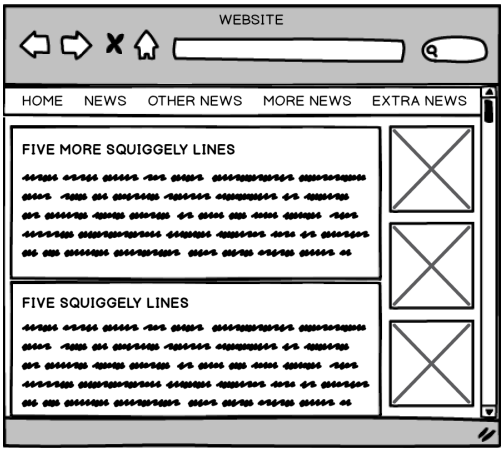

Figure 7. The user does not have an ad blocker installed (anymore) and has access to the site...

A user who is merely seeking additional information by clicking on the privacy policy link should not be considered as having agreed to the terms presented in them. However, if publishers also display a consent banner (Option 1) that informs users when reading the privacy policy that further use of the website will be considered consent, a user who continues using the website after accessing the privacy policy should be considered as having agreed to the privacy policy. The privacy policy should also provide information and a way to withdraw consent, but publishers may refuse access to their website to those users who do not consent or withdraw consent to their making use of ad blocker detection.

The disadvantage of a consent wall is that it interrupts the browsing experience of all users and not just those who are actually deploying an ad blocker. However, it allows a publisher to ensure that it is not possible for a user who has an ad blocker enabled to use the site before agreeing to ad blocker detection. In addition, if a publisher does not wish to restrict access and/or engage in a conversation with users of ad blockers, a hard opt-in may be over-kill compared to Option 1.

Combining Options 1 and 2

In order to minimize disruptions of the average user's experience, the two methods described in Options 1 and 2 could be combined and used to complement each other in different circumstances. This is particularly useful where a publisher wants to restrict access and/or engage in a conversation with those users who are using ad blockers.

The consent banner could be employed where visitors are accessing the homepage. This would minimize the disruption of the overall user experience, but still enable publishers to prevent users from accessing more content. This is because by further use of the website the user indicates his or her consent, allowing ad blocker detection scripts to be executed and users' access to the site to be restricted where appropriate.

The consent wall could be employed any time a first time visitor is accessing specific content without first accessing the homepage. This would mean a user could be prevented from accessing the content before he or she has consented to the use of ad blocker detection. This scenario may occur, for example, where a user arrives on a specific page by clicking on a link from another website, and does not take any other action which would constitute consent to the use of cookies and ad blocker detection.

In any case, publishers should combine consent requests for ad blocker detection and cookies to keep track of a user's consent status, and to avoid potentially disrupting the user experience for returning users.