e·capacity
Online Strategy and Execution

Whitepaper, v1.0

Adobe & ITP

Avoid being affected by Apple's Intelligent Tracking Prevention

Kasper Andersen
01-08-2019

Intelligent Tracking Prevention

What is ITP?

Intelligent Tracking Prevention (ITP) is a feature of the WebKit used by Apple to power its Safari web browser and was shipped in the new release of Safari 12 and iOS 11. It was released with the purpose of improving online privacy and reduce tracking.

ITP History Lesson and Releases

Background

Prior to ITP Safari desktop and mobile browsers blocked third-party cookies by default. This was done with the purpose of protecting users' online privacy, as third-party cookies are often used as trackers by AdTech platforms. As a work-around AdTech Platforms figured out a way to place a first-party cookie. When users clicked an ad, the user would be directed to the AdTech platform's domain, which would set a first-party cookie, then redirect the browser to the advertiser's landing page. Safari would then approve the third-party cookie, as it had already been used in a first-party context.

The release of ITP 1.0 and 1.1 was aimed to focus on these first-party cookies acting as trackers.

ITP 1.0

To avoid the use of a first-party cookie as a tracker, ITP 1.0 and 1.1 had a feature that allowed first-party trackers to behave like third-party trackers as long as the user visited the AdTech website within 24-hours. If the user didn't visit the AdTech website within 24 hours, the cookie cannot be used for ad retargeting and would have to display a non-retargeted ad to the user.

More on ITP 1.0

ITP 1.1

Changes were introduced to ITP 1.1, to make it easier to use third-party services that serve embedded content (e.g. embedded video, social logins, etc.). This was because ITP 1.0 defeated the whole purpose of embedded content, and basically required users to visit services in a first-party context before using widgets on a site.

To get round the limitations of ITP 1.0 & 1.1, some publishers implemented a unique query string aka retargeting script to internal URLs. This meant that when a user clicked an internal link on a publisher's website, they were first directed to the AdTech website and then back to the internal target URL. Consequently, visitors were often 'visiting' the AdTech website, allowing their first-party cookie to avoid being deleted after the 24 hour window.

More on ITP 1.1

ITP 2.0

On June 2018 ITP 2.0 was released and introduced major changes that seriously impacted reporting, affiliate marketing and attribution techniques.

The 24-hour grace period was removed and instead Storage Access API was introduced. This meant that third-party embedded widgets (like and sharing on e.g. Facebook) now have to request access to their first-party cookies when the user interacts with them on different websites. In other words, Safari throws a popup asking to allow or don't allow.

Another feature that was released is the ability to detect when a domain is used for creating redirects for the sole purpose of setting a tracking cookie. If such behaviour is detected the domains will have their cookies deleted.

Both Google and Facebook have come up with some solutions to address the changes in ITP 2.0 – Google has a site-wide tag and Facebook have released a first-party cookie option.

More on ITP 2.0

ITP 2.1

The most important change in ITP 2.1 is the 7-day expiration for cookies. It is important to understand that cookies can be set in two ways:

1. Client-side using document.cookie API
2. Server-side using HTTP response method set-cookie

For the 7-day expiration, only client-side cookies are affected by the update, which include the Adobe and Google Analytics cookies as these cookies are set via the JavaScript library (More on that in the next section).

More on ITP 2.1

ITP 2.2

Only 2 months after the release of ITP 2.1, WebKit announced a new version (ITP 2.2), which is focused on cross-domain tracking with link decorating. Link decoration is when you're adding a query string (domain.com**?clickID=124**) parameter or a fragment identifier (domain.com/**#clickID124**).

This is commonly used to track external campaigns but can also be used to pass information to other sites, as it enables them to persistently track a person on those sites. This practice is called cross-site tracking via link decoration. This is what Apple is addressing with ITP 2.2.

If a cookie is set client-side, AND the referrer has been identified as having cross-site tracking capabilities and the URL contains link decorating, the cookie will be limited to 1-day, instead of 7-days.

More on ITP 2.2

Adobe Experience Cloud

Is ITP affecting Adobe implementations?

ITP versions from 1.0-2.0 had little to no impact on Adobe solutions and data collected. Only implementations that are using the old tracking server ending with *207.net*, are impacted (legacy s_vi cookie). The 207.net domain is back from the Omniture days, so only really…as in really old implementations would be using this tracking server.

The real problem occurred with ITP 2.1, as it is limiting the VisitorID cookie (AMCV cookie) to 7 days. Without ITP the expiration would be set to 2 years.

Am I impacted?

As a rule of thumb, you're primarily impacted if you have a high number of visitors from mobile devices or if your visitors return frequency is higher than 7 days.

According to statcounter.com, for Denmark, Safari browser on desktop represents 14% and for mobile it is 50%[1]. Adobe says that across their customer base, approximately 20% of total web traffic occurs on Safari. For mobile browser data collection, closer to 50% occurs on Safari.

How is my solution/data impacted?

Adobe Launch & DTM

DTM uses first-party cookies that are set client-side to persist data elements, which will be limited to 7-days. Also, if you're using custom code to set cookies, then these will also be affected by the 7-day restriction.

Launch relies on local storage for persistence of data elements and is not affected by the changes introduced by ITP 2.1.

> ⓘ **Note**
> DTM is being sunset over 3 steps. First step was July 2019 and have already taken place. If you don't already have a plan in place to migrate to Adobe Launch, then now is the time.

Adobe Analytics (AMCV cookie)

Due to the cookie lifetime being reduced to 7 days, you may experience an increase of unique visitors coming from Safari browsers. Visit and page views should not be impacted.

Adobe Target (MBOX cookie)

This is used for keeping track of the visitor profile, so target activities that look at the visitor profile may have a decreased lookback period.

[1] *Source*: statcounter.com

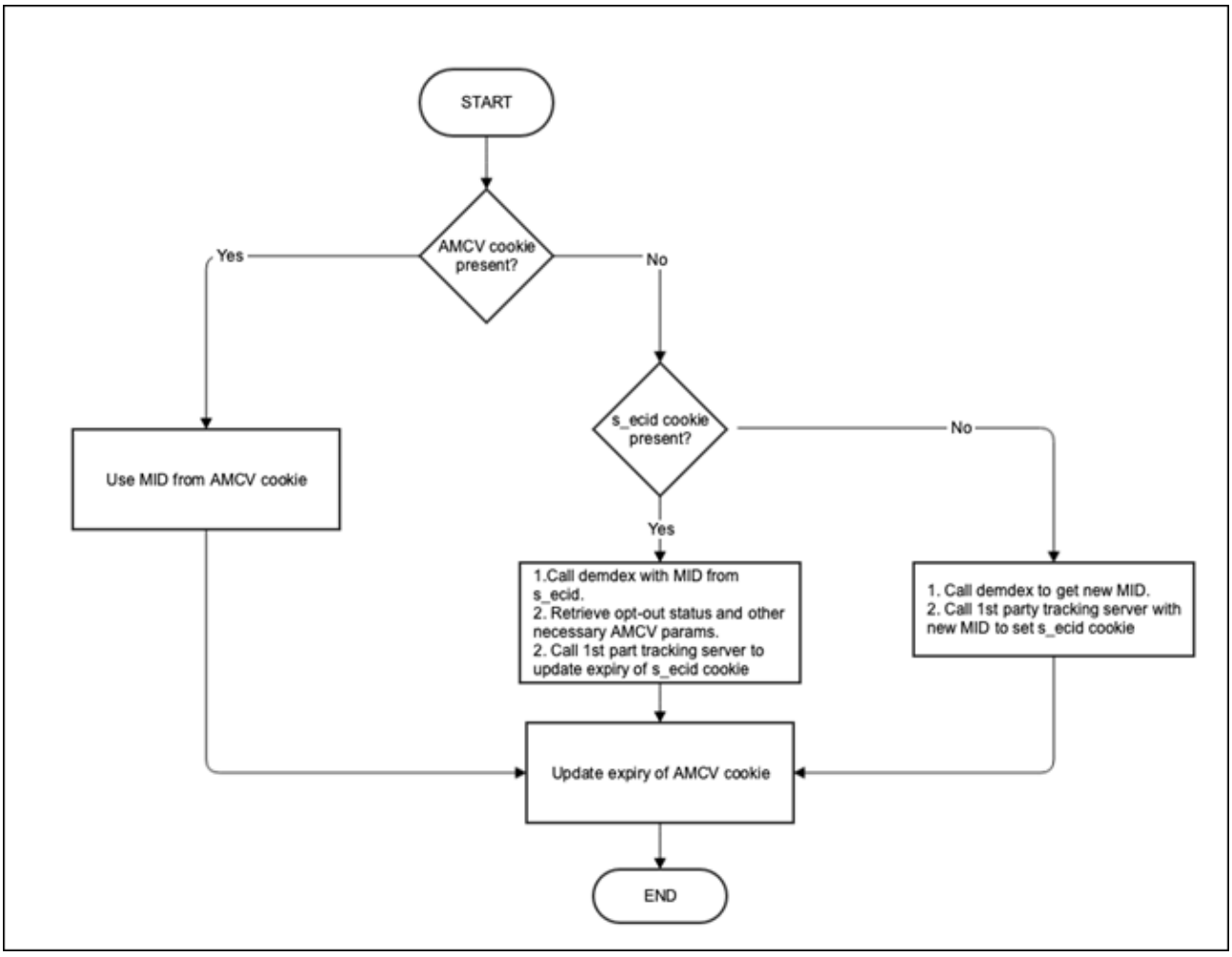
Adobe Audience Manager (DEMDEX cookie)

This is also referred to as the UUID cookie and contains a unique id for a site visitor; it is used by Audience Manager for visitor identification, ID synchronization, segmentation, modelling, reporting etc. You may see a decrease in overall Addressable Audience. Total Devices and Average Number of Devices counts in the Profile Merge Rule reporting may increase, as device IDs are re-created and synced more frequently in Safari.

The solution

As only client-side cookies are affected by the change, the solution is to move your cookie to server-side. Adobe announced June/July '19 that they introduced changes to their CNAME tracking servers, which are setting the ECID in a first-party cookie, set server-side.

Once a request is made to the Adobe Visitor ID Service and an ECID is retrieved, a server-side cookie named, s_ecid is set. This is how it works:



Source: https://docs.adobe.com/content/help/en/id-service/using/reference/ecid-library-methods.html

Requirements

In order to take advantage of this it requires that you're on ECID library (visitorAPI.js) v. 4.3.0+ and are using a CNAME record in your deployment aka. Adobe Managed Certificate Program.

How to get started

1. Make sure you ECID library has been updated to the before mentioned version or higher.
2. Start the CNAME process by opening a ticket with Adobe Customer Care. They will ask you to fill out a form.
3. Adobe Customer Care will then provide your CNAME values, which you will have to create on your DNS server
4. Once Adobe confirms that the changes have been applied in production and you have the CNAME records installed, you can update your s.trackingServer & s.trackingServerSecure variables, to ensure you're making use of the server-side cookie.

Questions

If you have any comments, questions or would like to discuss how you're impacted by ITP, then feel free to connect, ka@ecapacity.dk (+45 70 26 27 23).

More Resources

1. Experience Cloud ID Service, Release Notes: https://docs.adobe.com/content/help/en/id-service/using/release-notes/release-notes.html
2. ECID library methods: https://docs.adobe.com/content/help/en/id-service/using/reference/ecid-library-methods.html
3. Adobe Managed Certificate Program https://marketing.adobe.com/resources/help/en_US/whitepapers/first_party_cookies/adobe_managed_cert_pgm.html
4. Data Collection CNAMEs and Cross-Domain Tracking https://docs.adobe.com/content/help/en/id-service/using/reference/analytics-reference/cname.html
5. Adobe Target & ITP: https://medium.com/adobetech/keep-on-personalizing-adobe-target-supports-apple-safaris-itp-policies-for-cookies-bobab20696c0
6. ITP 1.0 https://webkit.org/blog/7675/intelligent-tracking-prevention/
7. ITP 1.1 https://webkit.org/blog/8142/intelligent-tracking-prevention-1-1/
8. ITP 2.0 https://webkit.org/blog/8311/intelligent-tracking-prevention-2-0/
9. ITP 2.1 https://webkit.org/blog/8613/intelligent-tracking-prevention-2-1/
10. ITP 2.2 https://webkit.org/blog/8828/intelligent-tracking-prevention-2-2/