Intelligent Tracking Prevention and Ad Blocker Technical Guide

Sitecore Discover

ITP and Ad Blocker Technical Guide Document V 1.0.5 20201111

Table of Contents

Chapter 1 Introduction

User privacy on the internet is a growing issue with policymakers and companies across the globe. In the last few years, two main developments have occurred:

1. Apple announced the rolling out of Intelligent Tracking Prevention 2.0 (ITP 2.0) in its Safari browsers.
2. Ad Blockers have become very popular and sophisticated. They can dynamically detect and block third-party domains that track user activity on your website.

In this guide, we discuss the impact of the above and Sitecore Discover's solution to minimize the impact on your users.

Chapter 2 Intelligent Tracking Prevention 2.0

Intelligent Tracking Prevention (ITP) 2.0 is a proposal by Apple to limit the life of third-party cookies on websites accessed using the Safari browser. It requires users to grant permission to third parties to track their activity on the site. A third party is any domain that is not the domain from which the page has been served. Some common third-party services used by websites include Google Analytics, Omniture, and any other service provider that you may use, including Discover.

You can read the details of the proposal at Webkit.org.

Firefox has also announced that it will block third-party cookies by default. See this article for more information.

The key points about ITP 2.0 are:

- Third-party cookies are dead. Cookies must be on the first-party domain, i.e., the customer's domain.
- Even on first-party domains, the cookie will be blackholed (purged) if the user doesn't visit the customer's website in 30 days.
- The referrer information will be truncated to only the fully qualified domain name, i.e., the referrer will only be the domain name without any query parameters.

Chapter 3 Intelligent Tracking Prevention 2.2

In 2019, Apple further updated the ITP specifications in version 2.2. This version limits cookie life to one day if the following two conditions are met:

1. The user navigated to the current website from a domain classified with cross-site tracking capabilities.
2. The final URL of the navigation mentioned above has a query string and/or a fragment identifier.

You can read more details about version 2.2 at Webkit.org.

Chapter 4 Intelligent Tracking Prevention 2.3

Apple updated the ITP feature again in version 2.3. ITP 2.3 aims to eliminate a workaround that enables companies to track people on other companies' sites without relying on cookies. Instead of storing the tracking IDs within a first-party cookie, they use non-cookie-based web storage mechanisms, such as local storage.

ITP 2.3 works by marking non-cookie website data for deletion if a user navigates from a domain classified with cross-site tracking capabilities to a URL with a query string or fragment identifier. If the user then uses Safari for seven days without interacting with that website, all the non-cookie website data is deleted.

Example:

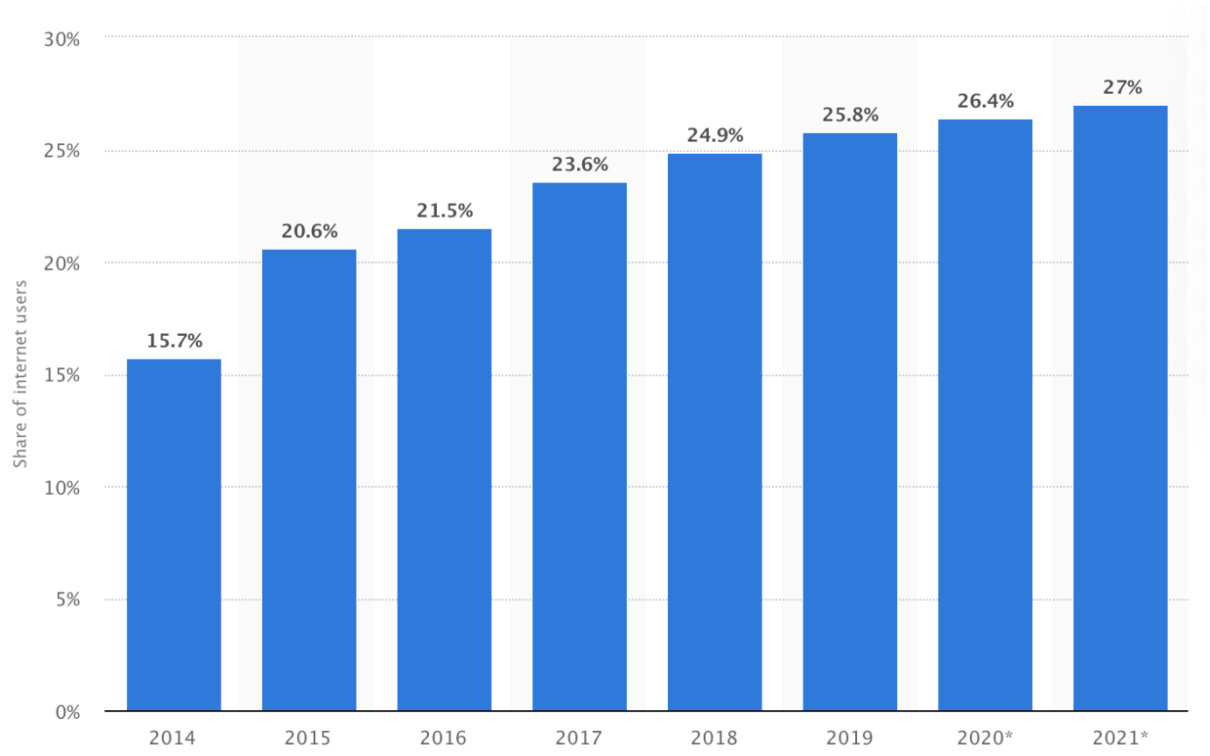
1. A user is navigated to `website.example` from a domain with cross-site tracking capabilities. The final URL is `website.example?clickID=0123456789`.
2. Seven days of Safari use later, the user has not returned to `website.example`, so Safari deletes all the non-cookie website data.

You can read more about ITP 2.3 at Webkit.org.

Chapter 5 Ad Blockers

In recent years, ad blockers have become very sophisticated and are able to dynamically detect third-party domains to block any tracking activity.

As they have become more effective, ad blockers have also gained in popularity. According to Statista.com, it was found that 15.7% of U.S. internet users blocked ads on their connected devices in 2014. This figure is projected to grow to 27% in 2021. See the following graph showing the user penetration rate of ad blockers.



Chapter 6 Effect on Discover Services

The Discover Service specializes in using sophisticated personalization technology to significantly improve your revenue. To personalize search results, generate recommendations, send relevant selective emails, and provide deep user insights, Discover must monitor user activity on your website while also serving search results and recommendations. ITP 2.3 and ad blockers do not have provisions to distinguish if a third party like Discover is a genuine third party providing valuable services to customers.

Since Discover services are accessed on your website using one of Discover's domains, it is considered a third-party service as it doesn't originate from the same domain as your website.

It is possible that portions of the website powered by Discover may not work properly or may not be personalized for users who are accessing your website from Safari, Firefox and other browsers who implement ITP 2.3. Further, Discover Services may not work at all if a user has installed an ad blocker like uOrigin, uOrigin Block, AdBlock Plus, etc.

Chapter 7 Solution

As explained above, cookies are blocked when the domain of a third-party service is different from the customers' domain.

The good news is that Discover stores cookies on the customers' domain. After setting up your subdomain, Discover will serve all requests and report events via your subdomain (which may look like **`rfk.`**`customerdomain.com`).

Further, Discover is not a destination site and users do not come to Discover. They directly visit your site and Discover only provides services on your site directly. Hence, ITP 2.3 does not affect the Discover experience.

This eliminates all issues addressed in this document.

7.1 Delegation Strategy

For Discover services to work as intended, we need to be able to serve traffic as if we were you. The first step in this process is to define a subdomain format. This subdomain will be used to delegate to nameservers provided by Discover. To do this, you may choose from one of the following strategies.

7.1.1 Strategy 1: Subdomain Delegation

Delegate a subdomain like **`rfk`**`.customerdomain.com` to point to nameservers provided by Discover.

Example:

Nameserver Details

TYPE	HOSTNAME	VALUE	TTL
NS	rfk.roughcountry.com	ns-1126.awsdns-12.org	3600
NS	rfk.roughcountry.com	ns-1544.awsdns-01.co.uk	3600
NS	rfk.roughcountry.com	ns-284.awsdns-35.com	3600
NS	rfk.roughcountry.com	ns-689.awsdns-22.net	3600

7.1.2 Strategy 2: CNAME Delegation

Set up CNAMEs with subdomains like `<somename>.rfk.customerdomain.com`. Discover provides the CNAME entries to make.

Example:

CNAME Details

TYPE	HOSTNAME	VALUE	TTL
CNAME	_380c9a97de0d2a0a08bae7ec5b27e707.rfk.calvinklein.ca.	_1b6ce256e589e26aef38bb73c7981aab.zbkrxsrfvj.acm-validations.aws.	86400
CNAME	rfk.calvinklein.ca	d5tl21p9o8sou.cloudfront.net	3600
CNAME	calvinkleinca.rfk.calvinklein.ca	d5tl21p9o8sou.cloudfront.net	3600

Let Discover know your preference, and we will provide you with the appropriate information.

7.2 Customer Setup

The next step is for you to set up the subdomain nameservers or CNAMEs. Once you have set them up, you may verify that the setup is correct by searching for your domain's NS record or DNS record.

You may also execute the following command on your terminal:

```
$ host -t NS rfk.<customerdomain>
```

Example:

```
$ host -t NS rfk.riggsandporter.com
rfk.riggsandporter.com name server ns-1262.awsdns-29.org.
rfk.riggsandporter.com name server ns-1868.awsdns-41.co.uk.
rfk.riggsandporter.com name server ns-450.awsdns-56.com.
rfk.riggsandporter.com name server ns-709.awsdns-24.net.
```

7.3 Final Setup by Discover

Discover will do the final setup to enable use of your subdomain for accessing all Discover services. Once done, you will refer to all Discover services through the `rfk.<customerdomain.com>` URL.

7.4 Updating Hosts

To determine the hosts and paths to use for various Discover services using your subdomain, visit **Customer Engagement Console** > **Developer Resources** > **API Access**

In general, you will update:

- the Discover beacon path
- the API host for both requests and events (if using Discover APIs)
- the page host (if using Discover hosted pages)