THESSALONIKI
digital analytics
MEETUP

WEB ANALYTICS & DATA PRIVACY

Panagiotis Tzamtzis, Head of Data-ops @ baresquare.com
Digital Analytics Meetup, Thessaloniki #20

PERSONAL DATA PROTECTION

PRIVACY

The individual's right to keep his or her data to himself or herself

CONFIDENTIALITY

The principle of keeping secure and secret from others, information given by (or about) an individual in the course of a professional relationship

SECURITY

The ability to keep data safe from unauthorized access

DO WE NEED ONLINE TRACKING?

1) *The web is dumb!*
2) *The web runs on ads*

What is online tracking used for, besides ads:

- Fraud prevention
- Personalization
- Data exchange between websites
- Bot detection
- Performance tracking
- Helping websites remember settings

TRACKING MECHANISMS

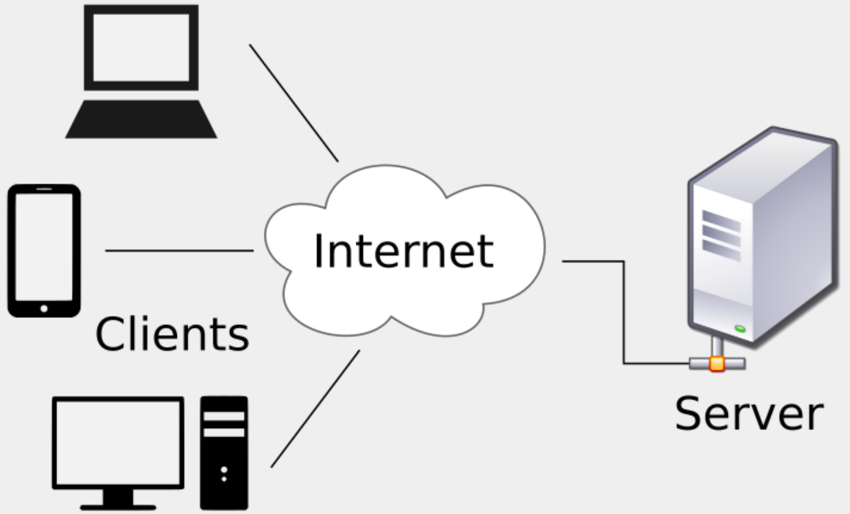
WHAT ? HOW ? WHY ?

- Cookies
- Localstorage / Sessionstorage
- Link decoration
- User accounts - Login
- Server-side tracking
- Shared device databases
- Fingerprinting
- Unique identifiers / interactions

(SERVER-SIDE VS CLIENT-SIDE)

CLIENT SIDE

Everything that gets executed / stored on the device used to browse the web (e.g. JavaScript)



SERVER SIDE

The data which get processed by the server and then get presented to the client in a static format
(e.g. PHP)

COOKIES

Small files (up to 4096 bytes) specific to each root domain stored client-side

Cookies were created 25 years ago to allow web systems remember (e.g. visited links)

Important difference between 1st party & 3rd party cookies!
1st party: Cookies under the domain you are visiting (e.g. save preferences)
3rd party: Cookies created under different domains (e.g. retargeting ads)

Used in online tracking to **remember** visitors and also share visitor data with 3rd parties
(Used in online marketing to store an ID, unique to a specific visitor)

LOCALSTORAGE / SESSIONSTORAGE

Simple storing mechanism (key-value pairs) for text (limit per domain: 2MB - 10MB).
Stored values are specific to a subdomain

Can replace or work alongside cookies to make storage more persistent

Localstorage: Data is stored forever unless the user deletes them
Sessionstorage: Data gets stored until the end of the session

Used in online tracking to **remember** visitors on the same website
(Used in online marketing to store an ID, unique to a specific visitor)

LINK DECORATION

Text key-value pairs inside the URL:
http:s//example.com**?id=123&sid=456#visitor**

Used in conjunction with cookies and localstorage and could even replace it in some cases.

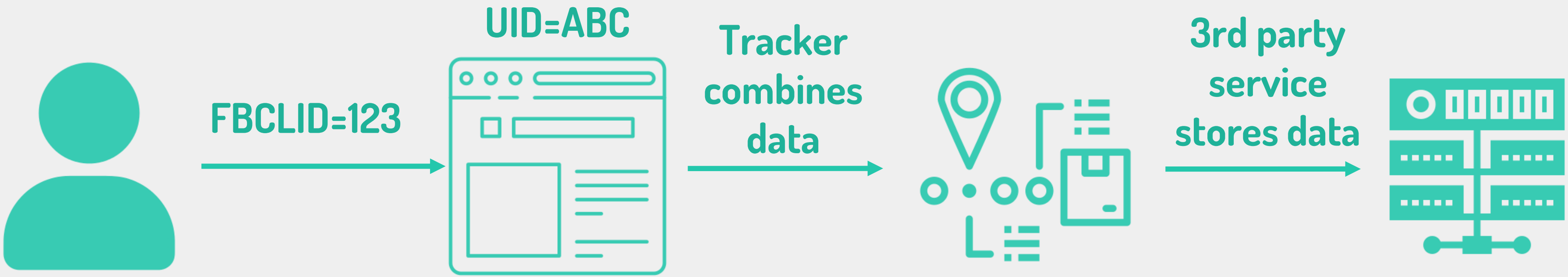
Used in online tracking to **share information** from one domain to another.
(e.g. when a website contains multiple domains, we can use link decoration to identify visitor consistently across multiple domains)

SHIFT TO FIRST PARTY COOKIES

3rd party cookies are not very usable anymore in marketing.

Online marketing technology is shifting to first party cookies, localstorage and link decoration to identify a visitor. Data is sent back to their servers using tags.

FACEBOOK TRACKING



USER ACCOUNT

Identifies visitors after logging in and combines profile data with web behaviour.

Eliminates the need of cookies and localstorage in most cases, as it can store information server-side.

Ideal when aiming for personalized experiences, **immune to anti-tracking** technologies today and works great across multiple devices.
(e.g. Amazon account)

SERVER-SIDE TRACKING

Combination of user account tracking and cookies/localstorage. Without having a user account, the website stores, server-side, all the information it collects.

Limited scope of information it can collect, partially immune to anti-tracking technologies. Still relies on cookies to identify visitors consistently. Combined with client-side tracking

Not widely used because of the dependencies it creates with the website's development process. Immune to adblocking and most anti-tracking technologies.

SHARED DEVICE DATABASES

Improves cross-device visitor tracking by sharing pseudonymized information across different companies and using a common device database. Relatively new concept in online marketing.

Dramatically reduces the time needed for a new website to provide uniform personalized experiences and to collect more meaningful web analytics data (Multi-channel attribution modelling).

Not widely used because of legal complications.
Example: Adobe Experience cloud device co-op (Available only in NA)

FINGERPRINTING

Queries for all publicly non-private available information and finds unique patterns allowing a website to identify a visitor on every session.

Examples of public information:

IP, Screen info, installed plugins & fonts, Time zone, user agent, battery information etc.

Very invasive technique which is not widely used in online marketing. Useful when trying to identify fraud and to protect accounts from unauthorized access.

UNIQUE IDENTIFIERS / INTERACTIONS

Uses information entered by the visitor (e.g. newsletter sign-up) or unique interactions (e.g. when calling to a unique phone number found on the website) to capture more detailed information. Similar to link decoration.

Useful when trying to **create a common key** between the online and offline presence of an organization or between 2 different channels.

Used in advanced implementations.
Difficult to manage and requires technical skills ETL tools

“Data that is loved, tends to survive”

KURT BOLLACKER, COMPUTER SCIENTIST

ANTI-TRACKING MECHANISMS

- DNT Do Not Track
- Ad-blockers / Tracking firewalls
- Legislation (GDPR, CCPA etc.)
- Safari ITP
- Firefox ETP
- Chrome SameSite

DNT (DO NOT TRACK)

A flag available in each browser's settings, indicating if the user wants to get tracked or not. This value is set to "false" by default (Tracking enabled).

Each website needs to be created in a way that is going to respect this setting and turn off tracking when DNT is set to TRUE.

GUESS WHAT! This setting is not monitored by most websites and is now considered obsolete...

AD-BLOCKERS / TRACKING FIREWALLS

Plugins / Extensions built to block either ads or tracking pixels.

A visitor / website owner selects the tracking pixels she wants to block and every time a call to that pixel's server is detected, it gets blocked (client-side).

Website owners can utilize them to control which tracking pixels are collecting traffic on their websites (especially useful for very large websites with multiple tags).
Visitors can have faster page load times, but these tools can only detect common patterns. Relatively easy to workaround the restrictions.

LEGISLATION

- **GDPR (25 May 2018)**
  Applies to data collected for EU citizens.
  Opt-in required before collecting data

- **CCPA (01 Jan 2020)**
  Applies to consumers in California
  Opt-out should be available when collecting private data

Both rules enhance the privacy, confidentiality, security and transparency of organizations working with personal data.

BROWSER MARKET OVERVIEW

APPLE SAFARI

Apple is profiting from mobile app sales and services targeted to Apple users. No real need for tracking technologies, justifies their “war”.

GOOGLE CHROME

Google offers tracking solutions (see Google analytics) and also profits from online advertising. It’s expected that Google Chrome will be less hostile against tracking solutions.

MOZILLA FIREFOX

Non-profit organization, offering a privacy oriented browser, with projects/funds aimed at changing how the world wide web operates (e.g. brave browser)

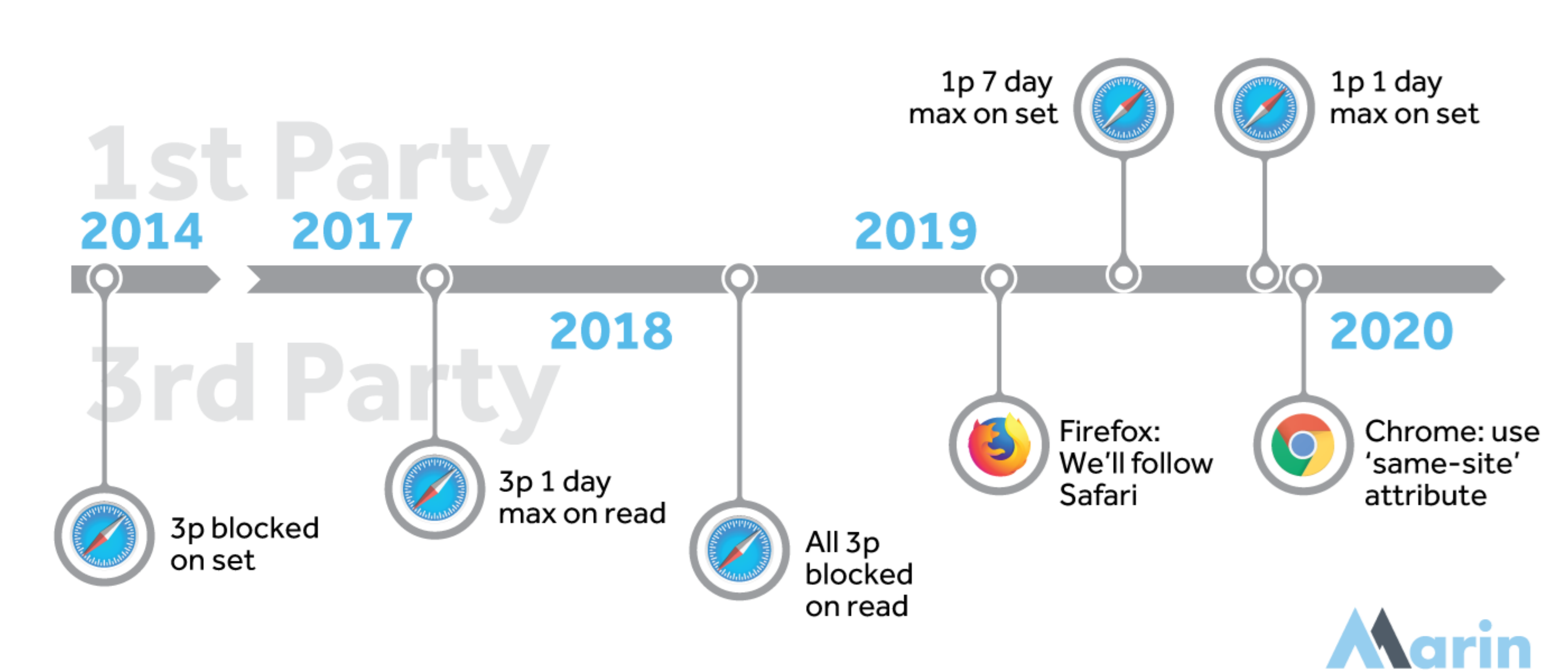
MICROSOFT EDGE

Microsoft is not putting a lot of effort lately on new browser features and just follows the bigger players.

OTHER BROWSERS

No need to pay attention unless you are managing a website spanning across multiple regions.

BROWSER ANTI-TRACKING TIMELINE

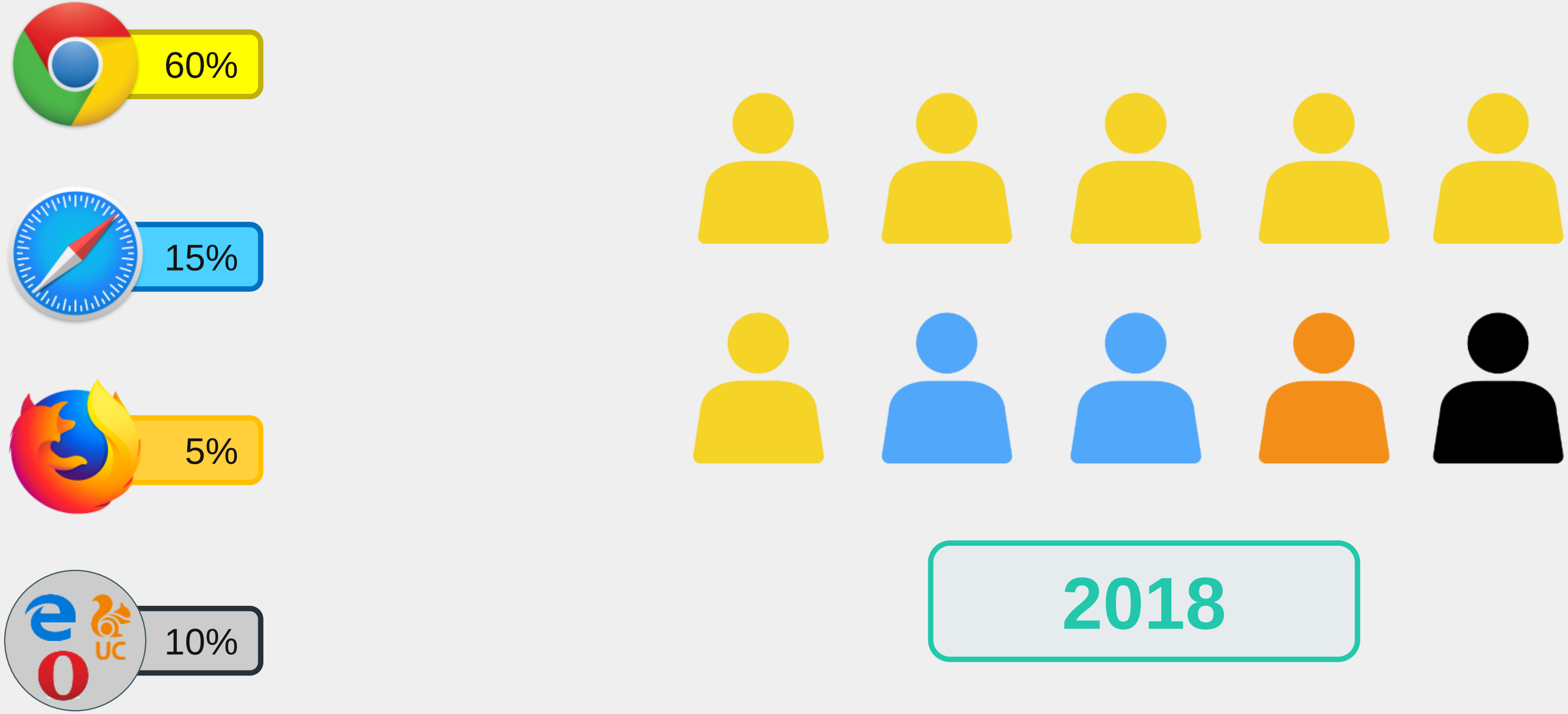


Timeline of major browser changes. Source: browser blogs

BROWSER TRACKING PROTECTION

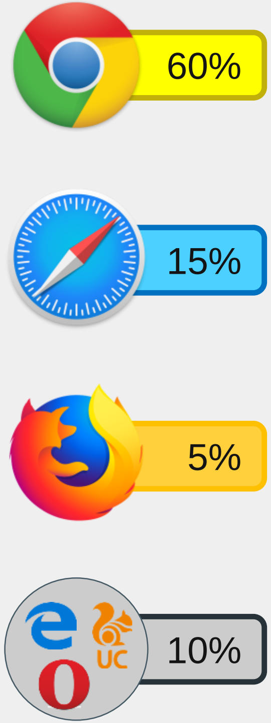
Browser	Market share	Release date	Web analytics impact	Online ads impact
Google chrome	? Quiz ?	Q1 2020 (SameSite)	Low impact	Medium impact on 3rd party Ads
Safari		Q2 2019 (ITP 2.2)	High impact (Accuracy limited to 7 days)	Retargeting limited to 1 day
Mozilla Firefox		Q3 2019 (ETP)	Low impact	Medium - High impact on 3rd party ads
Edge, Opera etc.		TBA	Low impact	Low impact on 3rd party ads

THE IMPORTANCE OF THESE CHANGES



2018

THE IMPORTANCE OF THESE CHANGES

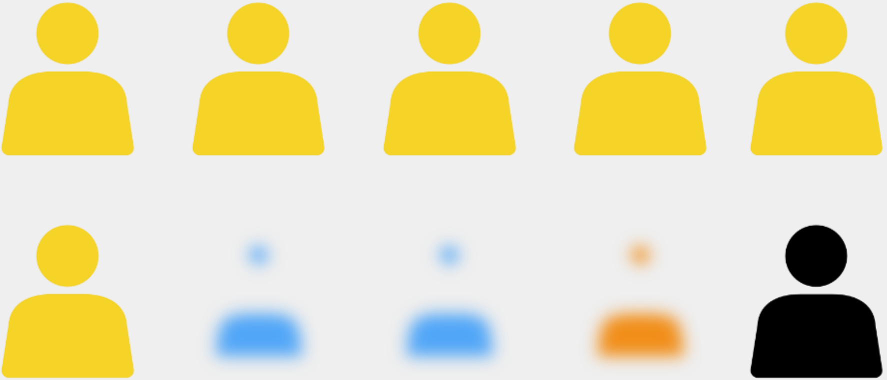


60%

15%

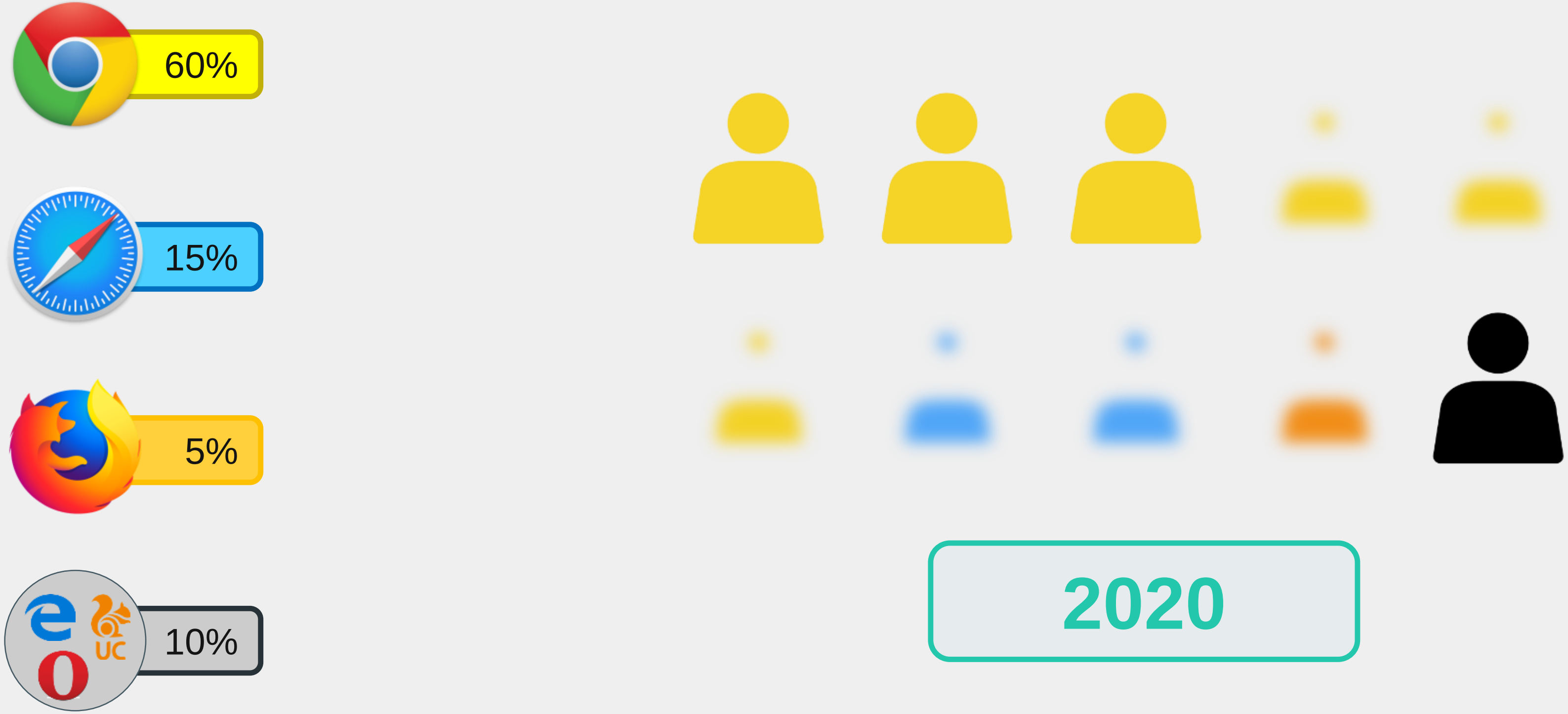
5%

10%



2019

THE IMPORTANCE OF THESE CHANGES



THE IMPORTANCE OF THESE CHANGES

3,5 εκατομμύρια επισκέπτες στο τον Ιούνιο - Πάνω από 4,5 εκατομμύρια τον Ιούλ

Web analytics accuracy

+

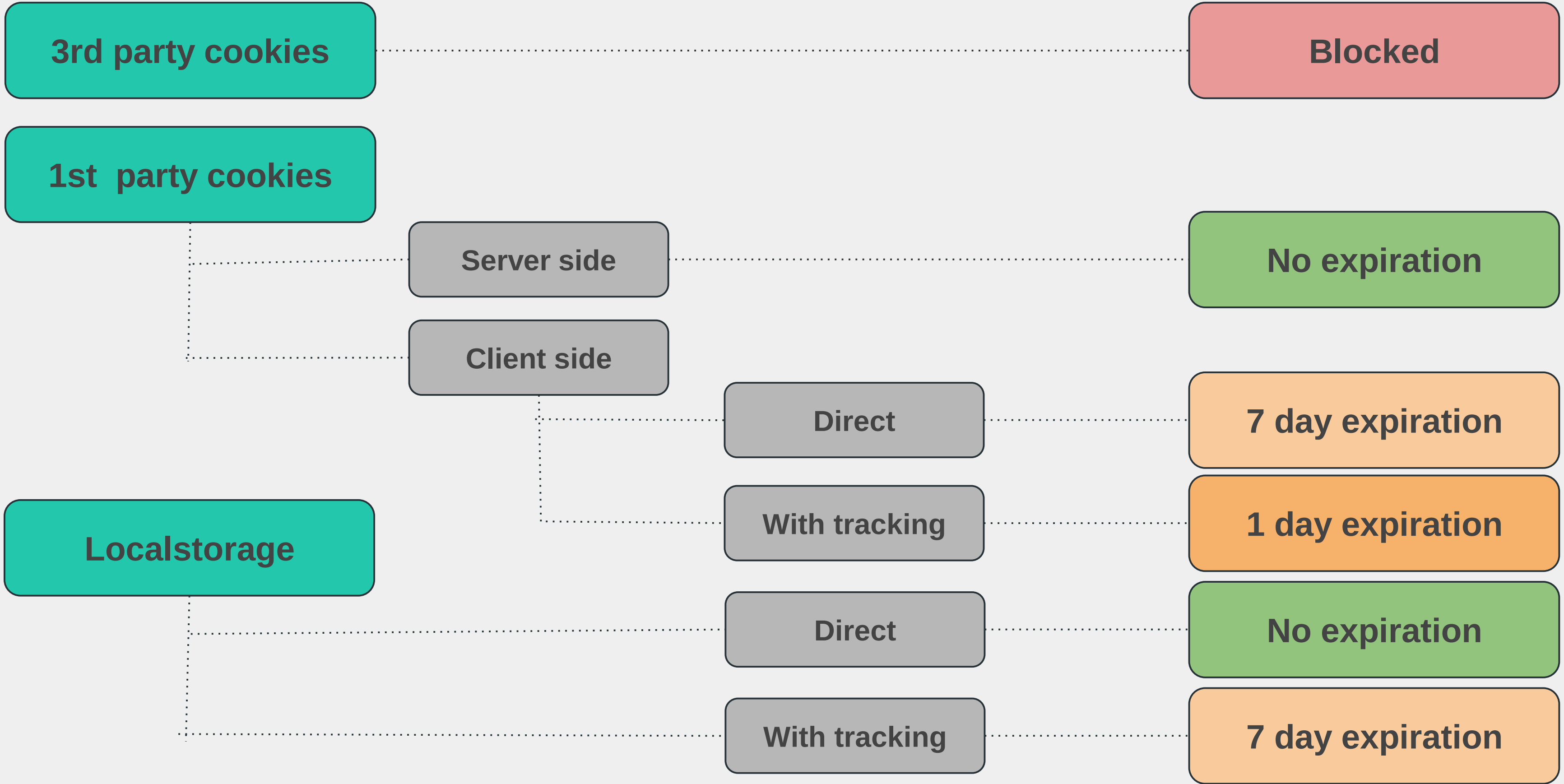
Essential web functionalities

183.102
154.178
1.020.000
Μοναδικοί επισκέπτες
ΠΗΓΗ ΣΤΟΙΧΕΙΩΝ
Google Analytics

SAFARI ITP

ITP Version	Client-side cookie expiration		Localstorage expiration	Safari Versions	Impact analysis	
	1st party	3rd party			Website analytics	Ads retargeting
1.0 (Jun 2017)	Unlimited	24h	Unlimited	Safari 11.0 OS X 10.11 macOS 10.13	Impacts only cross-domain tracking	Small impact
2.0 (Jun 2018)	Unlimited	Session	Unlimited	Safari 12.0 OS X 10.12 macOS 10.14	Impacts only cross-domain tracking	Very high impact on retargeting functionality
2.1 (Mar 2019)	7 days	Blocked	Unlimited	Safari 12.1 iOS 12.2 macOS 10.14.4	High impact on visitor identification	Very high impact on retargeting functionality
2.2 (May 2019)	1 to 7 days	Blocked	Unlimited	Safari 12.2 iOS 12.3 macOS 10.14.5	High impact on visitor identification	Very high impact on retargeting functionality
2.3 (Sep 2019)	1 to 7 days	Blocked	7 days (decorated links)	Safari 13 iOS 13 macOS 10.15	High impact on visitor identification	Very high impact on retargeting functionality

SAFARI ITP



3rd party cookies

Blocked

1st party cookies

Server side

No expiration

Client side

Direct

7 day expiration

With tracking

1 day expiration

Localstorage

Direct

No expiration

With tracking

7 day expiration

MOZILLA FIREFOX ETP

Current status:

- Blocks 3rd party cookies by default
- Blocks crypto mining scripts by default

Future updates:

- Blocking rules will be expanded to fingerprinting scripts

Low impact on web analytics accuracy and medium to high impact on retargeting.

GOOGLE CHROME SAMESITE

Q1 2020 updates:

- Blocking of fingerprinting scripts
- Plugin offering better visibility on displayed ads
- Cookies will need to indicate if they can be used as 3rd party to give visitors more control (SameSite flag)
- 3rd party cookies will only be accessible via HTTPS\

This approach will not be as hostile as Safari's ITP to online ads, but will cover every workaround for 3rd party cookies.

Web analytics is changing!
Prepare for an online world without cookies...

Want to learn more?

- Analytics power hour podcast
- Google chrome changes in more detail
- Safari ITP's impact on cookies webinar
- Gearing up for a cookie-less future presentation
- How anti-tracking affects analytics

THANKS

Panagiotis Tzamtzis
Head of data-ops @ baresquare.com
panagiotis@tzamtzis.gr
tzamtzis.gr

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**.