IAB Семинар 2024

Powerful Digital Leadership.

iab. bulgaria

Blagovest Iordanov

Founder & Managing Partner
ID – Digital Consulting

Privacy Sandbox

Голямата картина

Google Consent Mode V2

Малката промяна с огромен ефект за спазване на GDPR

iab. bulgaria

GOOGLE CONSENT MODE

Какво е:

Механизъм за управление на начина, по който Google конфигурира обработката на данните от различни (рекламодателски) инструменти на платформата.

Съставни елементи:

- Стандартизиран класификатор на съгласията: ad_storage, ad_user_data и прочие
- Команда “consent” на gtag.js API
- Транспортен механизъм - HTTP request параметри (dma, gcd, and gcs), подаващи стандартизирана информация за потребителското съгласие

Тагове и SDK, разпознаващи сигналите:

- Google tag (gtag.js)
- GA4, GA for Firebase SDK
- Google Ads
- Floodlight
- Conversion Linker

Имплементация:

- Basic Consent Mode – таговете не се изпълняват
- Advanced Consent Mode – таговете се изпълняват, с ограничени функционалности

GOOGLE CONSENT MODE V2

Промяната:

- Два допълнителни сигнала: ad_user_data и ad_personalization
- **Google вече изисква експлицитно подаден consent, за да активира нормалната функционалност на тагове и SDK.**


MYTHS AND
LEGENDS

ПЪРВА ЧАСТ

https://xplora.bg/google-ads-analytics/consent-mode-2-nai-vazhnoto-koeto-triabva-da-znaem/

„…от месец март Google започва задължителното налагане на Consent Mode V2…“

Google не налага Consent Mode в която и да е версия, нито е станало задължително сега. Всъщност, задължението на сайтове да събират съгласие на потребителите и да управляват според него изпълнението на различни инструменти (JS, <iframe>, <img> и пр.) имащи капацитет да събират и обработват потребителски данни е от началото на 2018 г.

“Consent Mode управлява бисквитките и предпочитанията на потребителите какви техни данни можем да събираме и как да ги използваме според регулациите на Европейския Съюз. Новата версия е обогатена с допълнителни параметри, които трябва да имплементираме в банера за бисквитки на сайта, както и в тракингите.”

Consent mode НЕ управлява бисквитките, а инструктира **ИЗКЛЮЧИТЕЛНО Google таговете** как да работят с бисквитки и подобни инструменти за маркиране на потребителите.
Consent mode НЕ управлява предпочитанията на потребителите, а е преносен механизъм на вече получени предпочитания.

Допълнителните параметри могат да се мапнат и с текущите цели, присъстващи в логиката за управление на съгласието на потребителите (т.нар. „consent banner”) и всъщност това е най-популярната имплементация – рядко се добавят нови цели.

„Advanced Consent Mode V2 (Разширен)
Google таговете се зареждат преди банера за съгласие да се зареди и когато потребителят откаже съгласие, таговете изпращат сигнали, които не идват от бисквитките (cookieless pings)“

Синхронната работа (едното зарежда преди/след другото) на две JS логики е сложно и рисковано предприятие. Това е очевидно, когато се имплеметира CMP логика събиране на съгласие чрез директно добавяне на JS библиотеката в Inline HTML.

Дори и при имплементация през GTM на зареждането на CMP библиотеките, препоръките са логиката за получаване на съгласие да зареди **ПРЕДИ** всички останали тагове. За целта Google добави специален GTM тригер – Consent Initialisation, който гарантирано минава преди всички останали тригери.

Имплементационната логика на gtag(„consent“) може да предвижда прочитане на запазените в бисквитка стойности на потребителското съгласие и да връща техните стойности на Default.
При Update, gtag.js ще съобрази начина на подаване на данните, без нужда от промени за Google таговете.

За всички останали тагове ще се наложи разработка на специфична логика за изпълнението им!

Сигналите не идват от бисквитките. Информацията, персистирана в тях е важна част от payload-а им.

ВТОРА ЧАСТ

https://netpeak.net/bg/blog/consent-mode-koyto-promeni-reklamiraneto-prez-2024/

„Обикновеният Consent Mode (CM) представлява банер, чрез който се спазват разпоредбите за поверителност на данните (GDPR). “

Мммм…не, визуалният интерфейс (банерът) е само част от Consent логиката.

“(Коментират Google Consent Mode V2) Тя управлява зареждането на таговете и скриптовете в нашия сайт.”

Не. Първо, GCM V2 управлява **поведението** на Google тагове.
Второ – касае **само работата на описаните Google** тагове и не управлява зареждането им на нашия сайт.

„В зависимост от направения избор сайтът ще изпрати сигнал дали и какви данни могат да се обработват от платформите Google Analytics и Google Ads.“

Сайтовете не могат да изпращат сигнали, но реализираната от нас логика може да го направи, през gtag.js

„Начини за интеграция на Google Consent Mode:
- чрез добавяне на статичен скрипт в кода на страницата, зареждащ се преди всички други скриптове;
- чрез имплементиране на Google Consent Mode в кода на сайта чрез Gtag или Tag Manager.“

Всъщност, могат да се използват и двата метода – напр. да инициализираме gtag(“consent”) чрез back-end функционалност, която анализира стойностите в бисквитката, отговаряща за записването на съгласието, след което чрез GTM Consent mode функционалностите да управлява **ОТДЕЛНО** засегнатите Google и останалите тагове.

Това е и препоръчваният от нас начин за имплементация, за да не зависи обработката на потребителските съгласия от Google Tag Manager.

ПРОВЕРКА НА ИМПЛЕМЕНТАЦИЯТА

Следим в JS конзолата какви са стойностите на параметрите от заявката.

gcd индикира съгласието по подразбиране

gcs може да приеме булеви стойности (1 или 0), маркиращи следното:

Value	ad_storage	analytics_storage
G100	Denied	Denied
G101	Denied	Granted
G110	Granted	Denied
G111	Granted	Granted
G1--	Did not require consent	Did not require consent

ПРОВЕРКА НА ИМПЛЕМЕНТАЦИЯТА

URL параметър **gcd** има следния формат:
&gcd=13<ad_storage>3<analytics_storage>3<ad_user_data>2<ad_personalization>5

Буква	Дефиниция
l (малко L)	Не е изпратен consent сигнал
p	denied по default, без update
q	denied по default и след update
t	granted по default, без update
r	denied по default и granted след update
m	denied след update, без default
n	granted след update, без default
u	granted по default, denied след update
v	granted по default, granted след update

ЕФЕКТИ ВЪРХУ ДАННИТЕ

GA4

iab. bulgaria

BASIC CONSENT MODE

Basic Consent Mode, без потребителско съгласие:

Таговете не се изпълняват.

Не се подават данни към никоя от Google платформите.

Приложим е само за описаните тагове от Google рекламодателската екосистема!

GA4 – ADVANCED CONSENT MODE

При липса на потребителско съгласие, gtag.js изпълнява т.нар. ”Cookieless pings”.

В тях липсва:

- user_pseudo_id (Client ID, стойността на _ga бисквитката)
- ga_session_number

C	D	E	F	N	O	P	
event_name	event_params.key	event_params.value.string_value	event_params.value.int_value	user_pseudo_id	privacy_info.analytics_storage	privacy_info.ads_storage	privacy_info.uses_tra
session_start	gtm_id	GTM-KMHCGS		22371403.1711506167	Yes	Yes	No
	batch_page_id		1711621657447				
	abandoned_cart	Undefined					
	batch_ordering_id		1				
	ga_session_number		3				
	ga_session_id		1711621658				
	gtm_version		397				
	ignore_referrer	true					
	session_engaged	0					
	page_title	Chaos: 3D Rendering & Simulation Software, featuring V-Ray					
	page_location						
session_start	page_title	Chaos			No	No	No
	abandoned_cart	Undefined					
	page_referrer			redacted)&firstName=RIYAZ&fullName=RIYAZ+GOURI&lastName=GOURI			
	page_location			)&fullName=RIYAZ+GOURI&return_to=https%3A%2F%2			
	ga_session_number		1				
	gtm_id	GTM-KMHCGS					
	ignore_referrer	true					
	batch_page_id		1711621642145				
	gtm_version		397				
	session_engaged	0					
	batch_ordering_id		3				

РЕЗУЛТАТ ВЪРХУ СУРОВИТЕ ДАННИ

Данни от потребители без съгласие:

- Хитовете престават да се обединяват в “Session“ и „User“
- Дефинициите, базирани на User и Session метриките не работят за тях
- Данните за придобиването се губят
- Атрибутирането не работи

Row	event_date	total_session_starts	empty_user_pseudo_
1	2024-03-10	18210	984
2	2024-03-09	18956	968
3	2024-03-08	26808	1478
4	2024-03-07	31054	1855
5	2024-03-06	32321	1955
6	2024-03-05	32753	1871
7	2024-03-04	31255	1784
8	2024-03-03	17994	958
9	2024-03-02	19269	1022
10	2024-03-01	28326	1563
11	2024-02-29	31096	1057
12	2024-02-28	32924	0
13	2024-02-27	33302	0
14	2024-02-26	30936	0
15	2024-02-25	17348	0
16	2024-02-24	18652	0
17	2024-02-23	27849	0

ПРЕДЛОЖЕНОТО РЕШЕНИЕ

Google Analytics behavioral modeling:

Механизъм за допълнителна обработка на данните, чрез device fingerpinting и сравнение на поведението на тези потребители с това на останалите.

Google Analytics conversion modeling:

„The term 'conversion' now aligns with how conversions are defined in Google Ads, addressing previous discrepancies across platforms. Important events previously labeled as 'conversions' in Analytics will be reclassified as 'key events.' These key events, when shared with Google Ads, will be considered conversions, facilitating more accurate performance measurement of ad campaigns and enabling better-informed marketing decisions.“

Maintain rigorous reporting

Modeled key events are only included when there is high confidence of quality. If there isn't enough traffic to inform the model, then modeled key events aren't reported (or, in the case of Google Analytics, are attributed to the "Direct" channel). This approach allows Google to recover loss of observability while also preventing over-prediction.

Don't identify individual users

Google doesn't allow fingerprint IDs or other attempts to identify individual users. Instead, Google aggregates data (such as historical key event rates, device type, time of day, geo, etc.) to predict the likelihood of key events.

Some countries require consent to use cookies for advertising activities. When advertisers use consent mode, key events are modeled for unconsented users.

Key event modeling covers both click-based events and engaged views for YouTube, to help with attribution for engaged-view key events.

Shot in the dark :

GA4 ще апроксимират, използвайки типичното процентно разпределение на действията на потребителите от извадката с налични данни върху извадката без.

Т.е. ако имаме 2% conversion rate за потребители от дадена география, устройство, браузър, тези коефициенти ще бъдат приложени върху набора хитове с идентични параметри.

Данните Ви ще получат по-голямо статистическо отклонение (по-ненадеждни) и отклоняващи се от тези в другите платформи.

Има идеи за решения, с потенциал да подобрят ситуацията.

ЕФЕКТИ ВЪРХУ ДАННИТЕ

Google Ads

iab. bulgaria

GOOGLE ADS CONSENT MODE MODELING

*"**Understanding what happens after you implement consent mode:***
In order to be able to meet our rigorous confidence thresholds, you'll need to meet the following quality checks:
- You have correctly implemented consent mode or the IAB Transparency & Consent Framework (TCF v2.0).
- You have a daily ad click threshold of 700 ad clicks over a 7 day period, per country and domain grouping.

"Once the above criteria are met, our models enter training periods. You can expect to gradually notice modeled conversions flow into your conversion reporting, and are likely to see gradual improvements in reported performance."

"When a user doesn't consent to ads cookies or analytics cookies, Consent Mode, using Google AI, adjusts the relevant Google tags' behavior to not read or write cookies for advertising or analytics purposes. Without cookies, advertisers experience a gap in their measurement and lose visibility into user paths on their site. They are no longer able to directly tie users' ad interactions to conversions."

"Conversion modeling may still be available to advertisers blocking cookieless pings, but our systems will be unable to generate advertiser-specific calibration factors, which may impact modeling accuracy Cookieless pings are critical to generate custom calibration factors for each advertiser."

GOOGLE ADS ONLINE CONVERSION MODELING

"When Google surfaces modeled conversions in Google Ads, we're predicting attributed conversions. In most cases, Google will receive ad interactions and online conversions but is missing the linkage between the two. Our modeling determines whether a Google ad interaction led to the online conversion. It doesn't determine whether or not a conversion happened."

"Regulations in some countries require that advertisers obtain consent for use of cookies related to advertising activities. Advertisers who have adopted consent mode will experience conversion modeling in line with their unconsented users. Conversions are modeled for unconsented users."

*"**Rigorous thresholds for reporting***
We only include modeled conversions in our reporting when we're highly confident that conversions actually occurred as a result of ad interactions. We avoid systematically reporting more conversions than reality and always aim to minimize over-reporting. This means for some users, we don't observe enough conversions on a regular basis to be able to confidently model. In these cases, we don't report any modeled conversions."

*"**Automatic integration***
Where we can accurately do so, Google will use available data to provide integrated conversion modeling in your conversion reporting and optimization. In some cases, such as when conversions cannot be observed for a set of users that hasn't consented to cookies, we'll need data about your consent rates so that we can provide conversion modeling."

Shot in the dark :

Отклоненията между данните и реалността ще станат по-големи. Съдейки по тенденциите през последните години, очаквам Google алгоритъмът да стане по-оптимистичен в атрибутирането на конверсии към Google Ads.

Това ще увеличи сумарната разлика между конверсиите от всички използвани платформи.

Google и Meta не популяризират възможностите за използването на 3rd party (техните идентификатори) данни, за да стимулират подаването на нашите (1st party) данни.

Когато наближи времето за премахване на бисквитките, очаквам да се окаже, че има алтернативни решения 😉

ДОПЪЛНИТЕЛНИ РЕСУРСИ

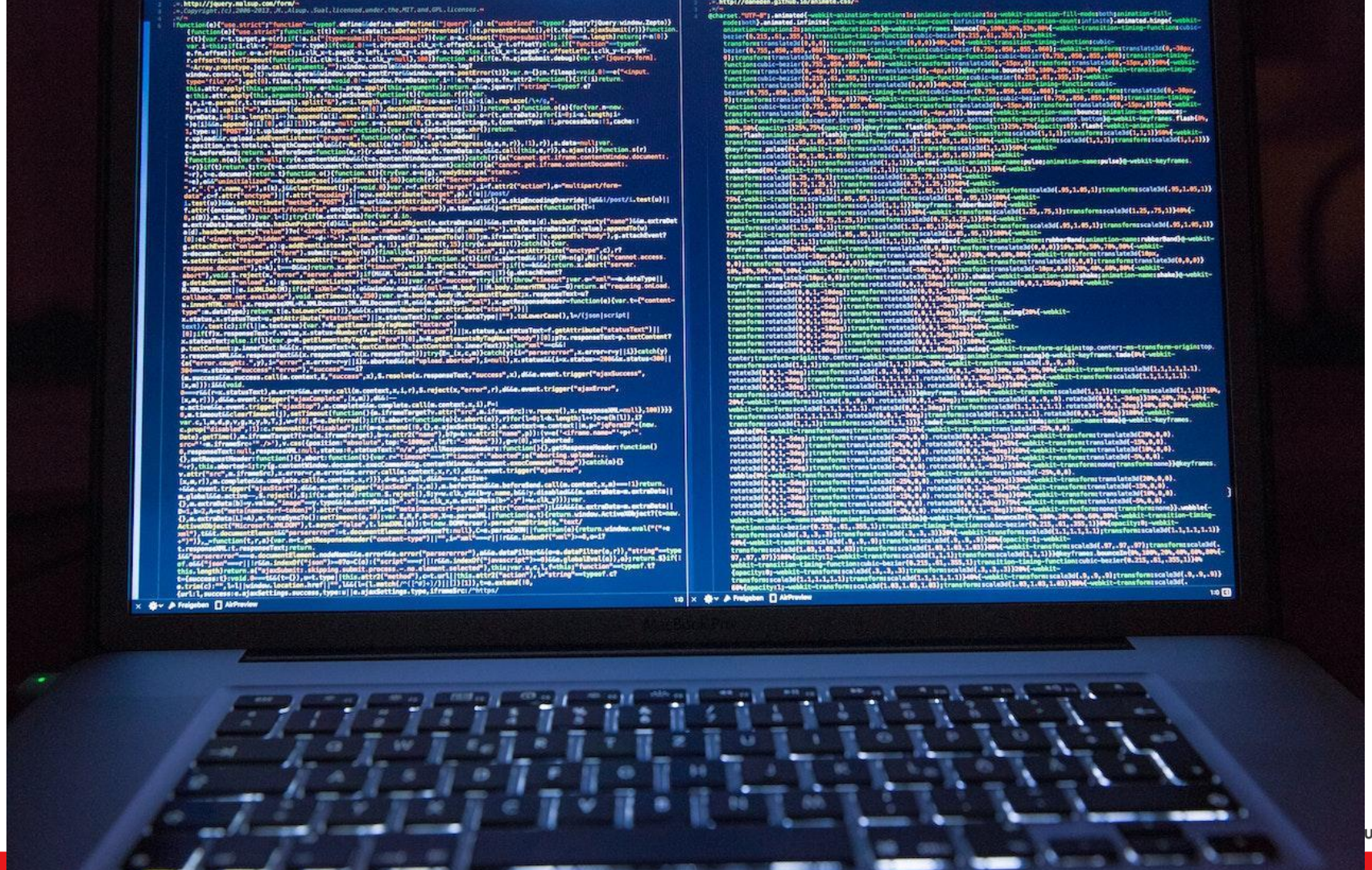
About consent mode

Consent mode overview

Google tag API reference

Updates to consent mode for traffic in European Economic Area (EEA)

(Meta) Cookie Consent Resource



PRIVACY SANDBOX

ГОЛЯМАТА КАРТИНА

iab. bulgaria

ТОВА ПЪК КАКВО Е?

„The Privacy Sandbox introduces a set of privacy-preserving APIs to support business models that fund the open web in the absence of tracking mechanisms like third-party cookies.“

- ✓ Индустриална инициатива, целяща създаване на технологии способни да решават многожество use cases, при „запазване поверителността на интернет потребителите“
- ✓ Очакванията са тя да модифицира **W3C web standards** (нещо значимо!) в тази посока.
- ✓ Ще се прилага за WEB и Android. Част от браузърите не поддържат всички инициативи.

КАКВО БЯХА 3rd PARTY COOKIES

„Third-party cookies are stored by a service that operates across multiple sites. For example, an ad platform might store a cookie when you visit a news site.

First-party cookies are stored by a website itself.“

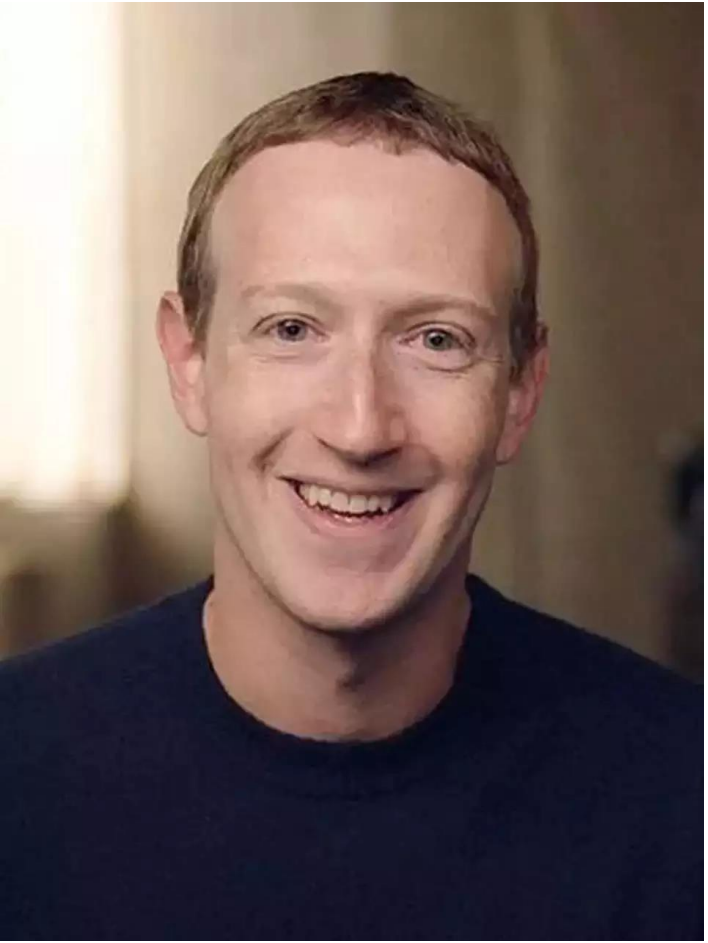
Със сигурност HTTP cookies не попадат в обхвата на инициативата.

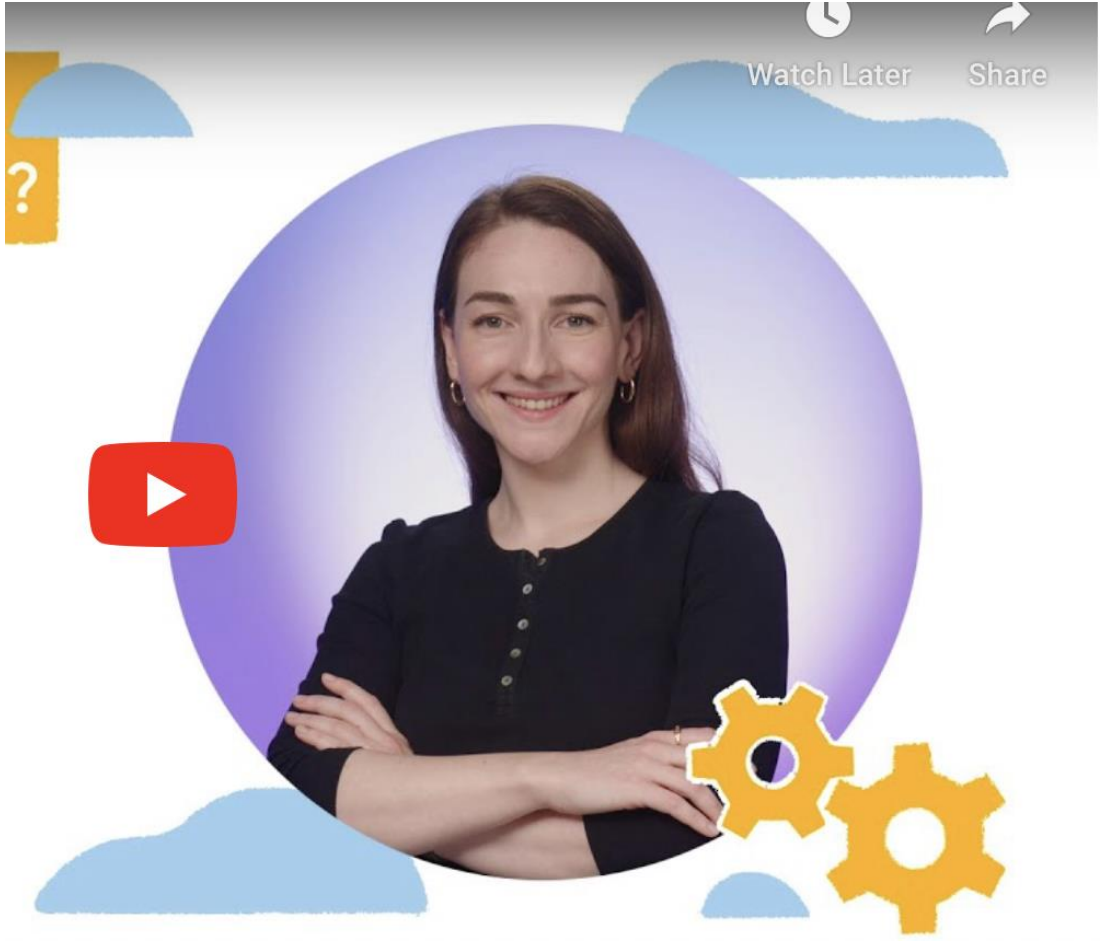
Всяка останала бисквитка, дори и записана от JS на Вашия домейн, ще бъде изложена на риск от блокиране.

КАК ЩЕ РАБОТИ ЦЯЛОТО НЕЩО?!

ОЧАКВАНИ РЕЗУЛТАТИ

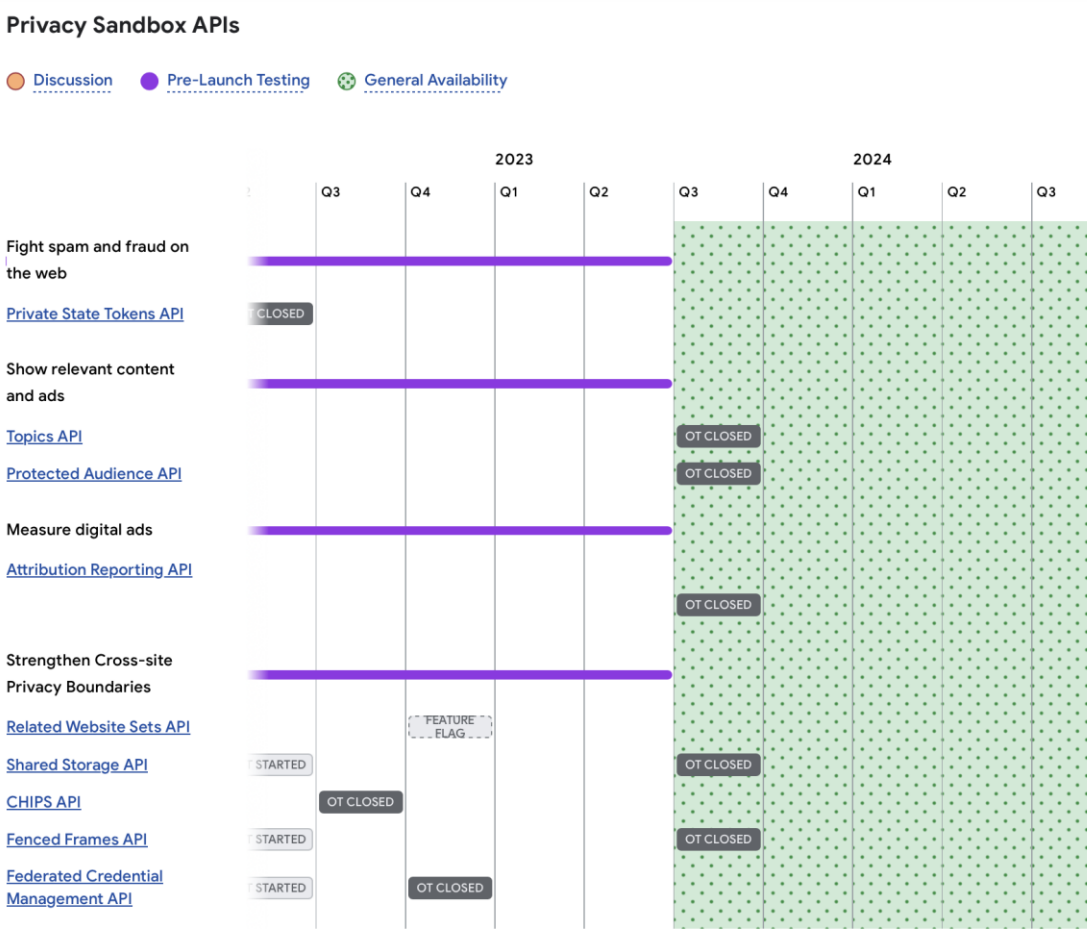
- ✓ Намаляване на общата ефективност на рекламата, с фокус: програматична, ремаркетинг, продуктови фийдове.
- ✓ GDN и Pmax ще понесат допълнително намаление на ефективността
- ✓ Промяна на позициите на рекламните платформи: най-облагодателствани са Meta (собствен login за всички потребители), Google Search (ясни потребителски намерения)
- ✓ Необходимост от допълнителни инвестиции за:
- Издатели – допълнителни настройки, добавяне на нови решения
- Рекламодатели – Напасване към новите изисквания, чрез анализ на платформените данни и модификации на рекламните стратегии и тактики




Watch Later
Share
?

ИНИЦИАТИВИТЕ

От няколко години се разработват решения, заместващи незаменимите бисквитки, под формата на набор от API.



bulgaria

БИЗНЕС ЦЕЛИ И ИНСТРУМЕНТИ

Бизне цели	Подходящ инструмент	Детайли
Измерване и атрибутиране на конверсиите	Attribution Reporting API	Click-through и view-through измерване Event-level и Агрегирани отчети
Сервиране на релевантни реклами	Protected Audience API (ex Fledge) – за ремаркетинг Topics API – за аудитория по интереси	Данните за потребителите се съхраняват от браузъра, вместо – от платформите. Създава coarse-grained теми, на база ML анализ на ниво hostnames 😂
Лимитиране на fingerprinting	Privacy Budget	Лимитира обема данни достъпен за JS, User-Agent header, Client Hints, device orientation и др.
Сигурност на IP адресите	Gnatcatcher предложение	Контролира достъпа до IP адресите
Борба със СПАМ и измами	Trust Tokens API	Потвърждаване на идентичността на посетителя без fingerprinting
Групиране на домейни, собственост на една и съща организация	First Party Sets	Дава възможност за деклариране на набор от 3rd party бисквитки като 1st party в рамките на дадена група домейни.

PROTECTED AUDIENCE API (ex-FLEDGE)

Целта на API е да осигури сервирането на remarketing и custom аудитории, но без да дава възможност на трети страни да получават информация за cross-site потребителското поведение. Дава възможност поддържаните браузъри да фасилитират on-device рекламни аукциони.

Механизмът на работа предвижда два набора от команди, за DSP и SSP. Всяка страна поддържа списък с key-value pairs, към които ще се обърне клиента (браузър/Android) в съответния момент (bid time – към DSP, ad score time – към SSP).

Браузърите поддържат метод, чрез който DSP/рекламодател може да бъде добавен в дадена група, негова собственост. Всяка група е браузър-специфична! **Важна особеност е способността сайтовете сами да дефинират групи от интерес.**

При посещение на издателски сайт, браузъра инициира аукцион, в който изчита наличните групи от интерес и се обръща към Key/Value services регистъра за информация чия собственост са, за да ги покани за наддаване. След това процесът е подобен на текущия – в отговора на заинтересуваните страни има предложение за цена и рекламни активи.

Браузърът зарежда активите на евентуалния печелившш и рапортува резултатт от аукциона. При евентуален клик се използва Fenced Frames Ads Reporting.

Advertiser* site A site that pays to advertise its products. bike-maker.example	**Ad-space buyer code**	**Site that displays ads** A site that gets paid for ad impressions. dailynews.example	**Ad-space seller code**	**Ad-space seller code**	**Ad-space seller code** and **Ad-space buyer code**
	`joinAdInterestGroup()`		`runAdAuction()`		`reportResult()` `reportWin()`
					
User visits advertiser site	Browser joins interest group	User visits site displaying ads	Ad auction run	Winning ad displayed	Results are reported
The user interacts with a site that wants to advertise its products. In this scenario, the ad-space **buyer** is likely to be a DSP or the advertiser itself.	The DSP (or the advertiser itself) makes a JavaScript call **`joinAdInterestGroup()`** asking the browser to add an interest group named `'running-shoes'` to those it belongs to.	The user visits a site that displays ads. The **seller** of ad space on the site is likely to be an SSP or the site itself.	The seller calls the function **`runAdAuction()`** to choose the most desirable ad based on seller code, bidding code from participating ad buyers, and realtime data from the **key/value service**.	The ad associated with the winning bid in the ad auction is displayed to the user in a **fenced frame**.	The seller's code can include a **`reportResult()`** function to report the auction outcome. Each buyer's code can include a **`reportWin()`** function.

*A publisher or adtech platform might also want to build interest groups.

КАЗУСИ

Изискване за K-anonymity – чрез алгоритъм се определя минимална граница, на която трябва да отговаря комбинацията от фактори:

✓URL на собственика на interest group

✓URL на наддаващия скрипт

✓URL на криейтива

✓Размер на рекламата (след 2025г.)

Комбинацията от фактори (tuple) трябва да била налична за поне 50 потребителя през последните 30 дни, като текущата имплементация е поставила тази стойност на 10 и е въпрос на следващо решение кога ще бъде мигрирана към 50.

ATTRIBUTION REPORTING API

Основната цел е да позволи атрибутирането на конверсиите без да се използват 3rd party бисквитки или прекомерен fingerprinting.

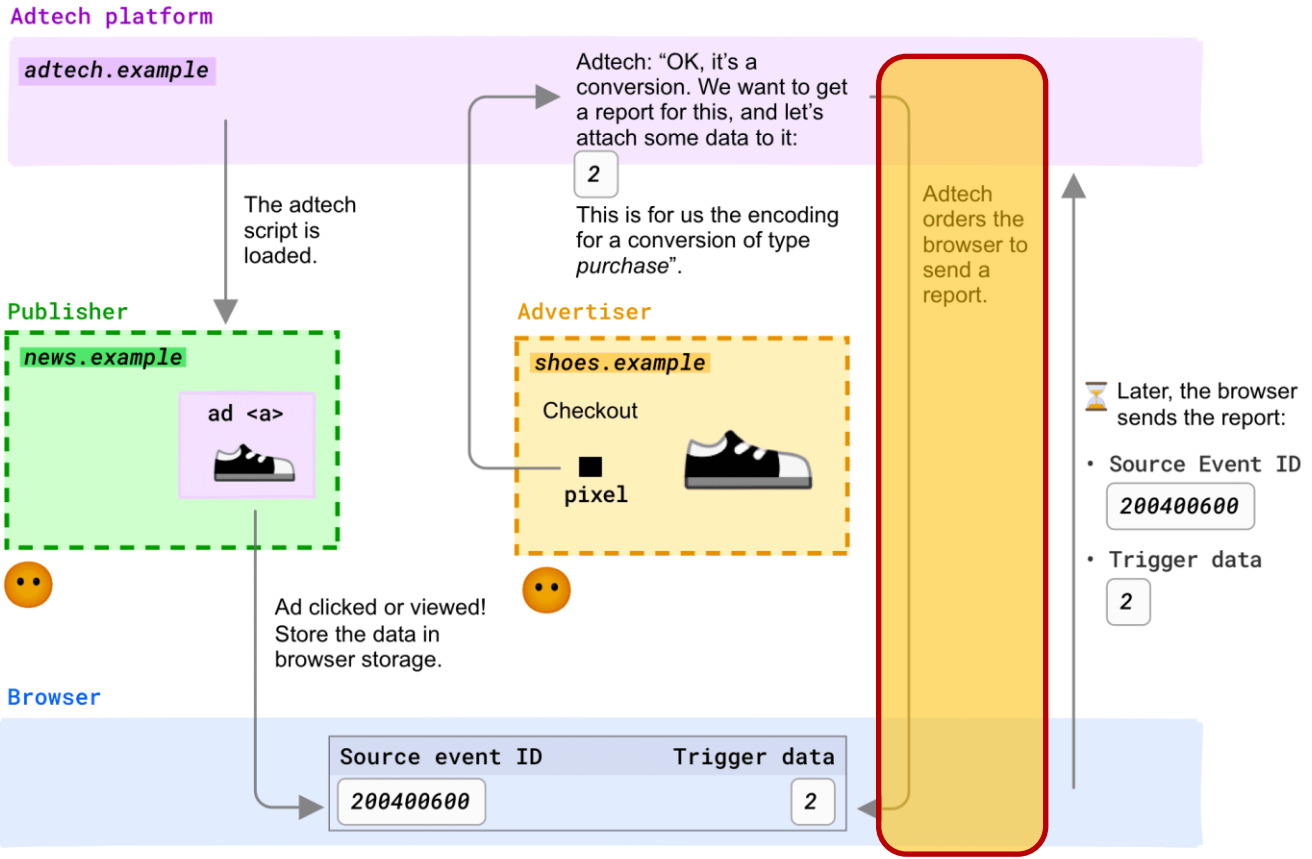
Добавеният шум (за получаване на по-груби данни) води до:

„The Attribution Reporting API may not be suited for cost-per-conversion billing needs, because of the noise added to event-level and summary reports“

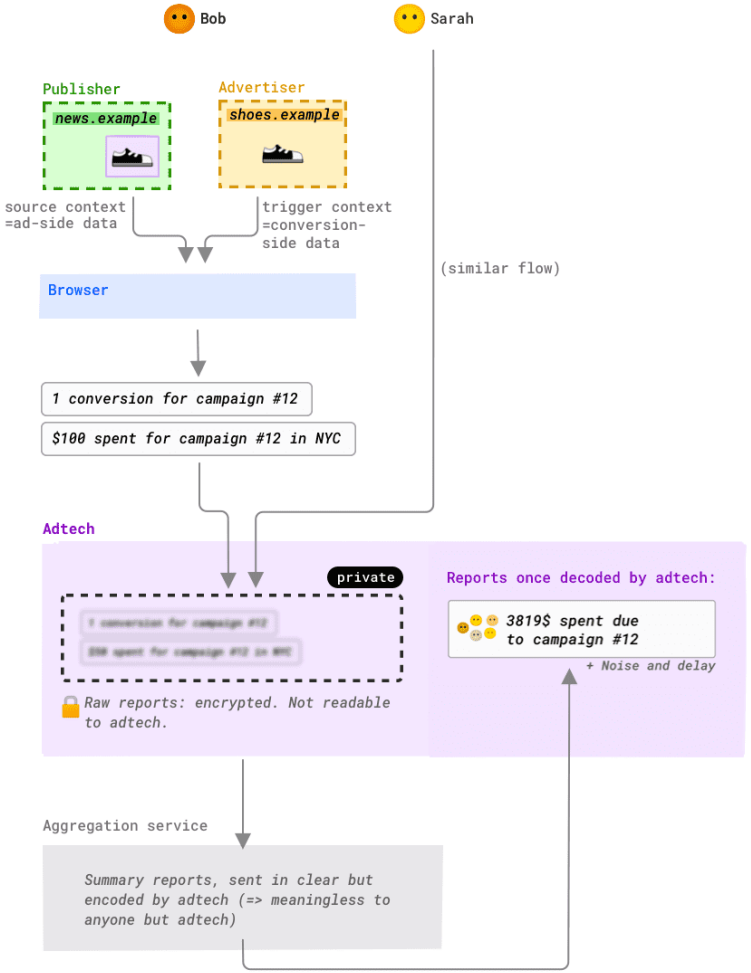
Поддръжка:
Firefox и Edge не са споделили сигнали

Safari и Webkit са негативни и няма да участват в инициативата, като предлагат собствена разработка - Private Click Measurement.

EVENT-LEVEL REPORTS



SUMMARY REPORTS



With third-party cookies: joined identity

User device private

(Nothing)

Adtech

Bob saw ad #200400
and bought red shoes size 8

Bob's activity and data on
news.example

AND*

Bob's activity and data on
shoes.example

*CROSS-SITE JOINT
OF DETAILED DATA
=> JOINED IDENTITY

Adtech

Event-level report:

Bob saw ad #200400
and bought something

+ Noise and delay

Bob's activity and data on
news.example

Summary report:

3819$ spent due
to campaign #12

+ Noise and delay

Raw report private

Bob's activity and data on
news.example

AND

Bob's activity and data on
shoes.example

Raw report: encrypted. Not
readable by adtech.

Aggregation service

private

1 conversion for campaign #12

$100 spent for campaign #12

Encoded by adtech. Not
meaningful to the trusted
servers.

КАЗУСИ

Добавен шум:

Добавеният шум (за получаване на по-груби данни) води до:

„The Attribution Reporting API may not be suited for cost-per-conversion billing needs, because of the noise added to event-level and summary reports“

Всеки е герой:

Какво ще стане, ако няколко платформи претендират за резултата от даден клик? А какво се случва с post-view арбитутирането? За Meta – ясно. Останалите какво ще правят?

Детайлност:

Потребителският идентификатор е 64-битов (ОК), но conversion идентификатора е 1 или 3 битов. В 3 бита можем да кодираме $2^3 = 8$ уникални стойности.

Забавяне:

Данните ще се изпращат с “известно“ забавяне, за да не се използват за поведенческо профилиране.

Поддръжка:
Firefox и Edge не са споделили сигнали

Safari и Webkit са негативни и няма да участват в инициативата, като предлагат собствена разработка - Private Click Measurement.

TOPICS API

Функционалност, предвидена да активира IBA (interest-based advertising) без да се използва гранулярно проследяване на потребителското поведение. Наследник на FLoC.

Начинът на работа предвижда възможност на API, чрез идентифициращи интереса статистически методи да предполага интересите на потребителите, на база страниците, които те посещават.

Част от механизма на работа е поддържане на информацията „свежа“, чрез концепцията за “Epoch”, представляващ релативен период от време (т.е. без да се знае началния момент), през който се събира информация за “User”, като допълнително на случаен принцип се избира една от петте най-популярни теми за периода. API caller (рекламна платформа), трябва да е заявил наблюдението на конкретна тема през най-актуалните 3 Epochs, за да може да я получи като информация. В отговор на заявката си, caller може да получи между 0 и 3 теми.

Коефицентът на рандомизиране е 5%, като има множество други ограничения за да се избегне възможността за профилиране (fingerprinting).

Таксономия, v.2 (471 записа)

RELATED WEBSITE SET (RWS)

Дава възможност на компаниите да декларират набор от сайтове, нейна собственост.

За тези сайтове поддържаните браузъри ще разрешават достъп до част от функционалностите на 3rd party бисквитките, за специфични цели.

Препоръчвам на по-големите издатели да проучат тази инициативата.

RWS Submission Guidelines

Canonical guidelines

SHARED STORAGE API

Функционалност, позволяваща cross-site достъп за запис, но лимитираща възможностите за четене.

По идея, браузърите трябва да разделят всички видове storage (cookies, localStorage, caches и т.н.), за да премахнат възможността за cross-site проследяване. Тъй като има бизнес цели, признати за „легитимни“ от инициативата, е разработен метод, позволяващ изключения.

За четенето на данни се използва специална среда, наречена *shared storage worklet*. В него JS може да извлича неразделена информация, но няма възможност да комуникира с външна страница.

Използването му е подходящо за следните цели:

✓Ротация на криейтиви

✓А/Б тестване

✓Custom UX

1. Buyer wins auction and needs to select an ad creative.
2. Buyer checks Shared Storage and finds user has not previously viewed or clicked for this campaign.
3. Buyer returns the globe ad. The user clicks on the ad.
4. Buyer updates Shared Storage variables.
5. For next ad win, buyer selects and displays the hotel creative.

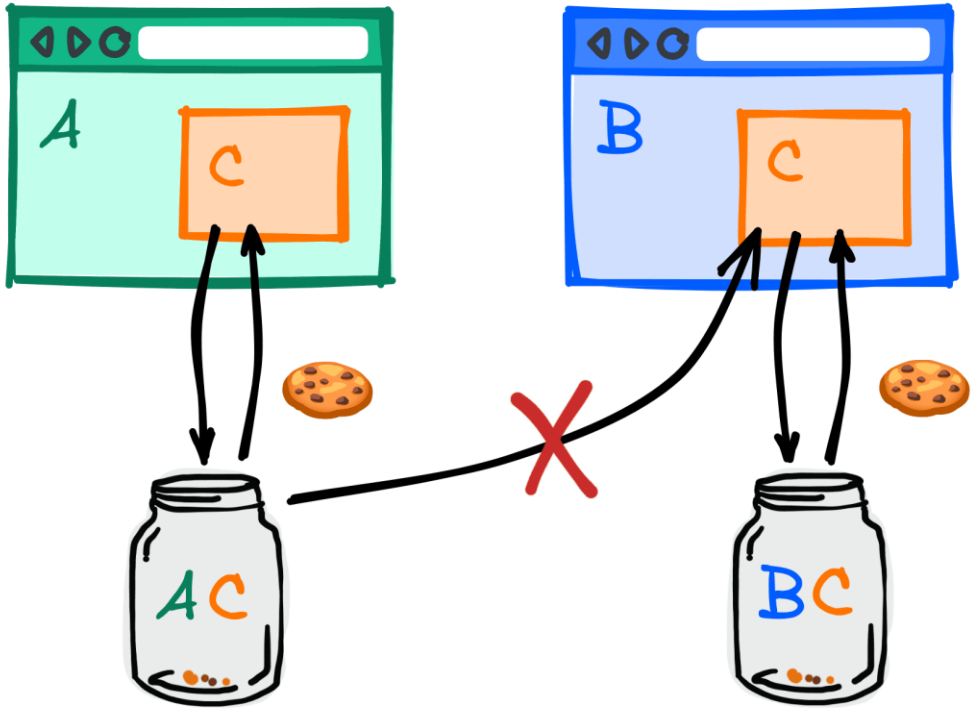
COOKIES HAVING INDEPENDENT PARTITIONED STATE (CHIPS)

По същество е начин за използване на 3rd party бисквитки. Позволява добавянето на бисквитки към partitioned storage и използване на двоен ключ за достъпването им.

Текущо бисквитките имат само един ключ, *host.* С внедряването на предложението, към него ще се добави нов ключ – *partition,* реализиран чрез нов cookie атрибут: `Partitioned`

Partitioned бисквитката се записва от 3rd party service, като може да се бъде прочетена от този service само на същия top-level domain.

Partitioned



A,B – top-level sites
C – embedded site

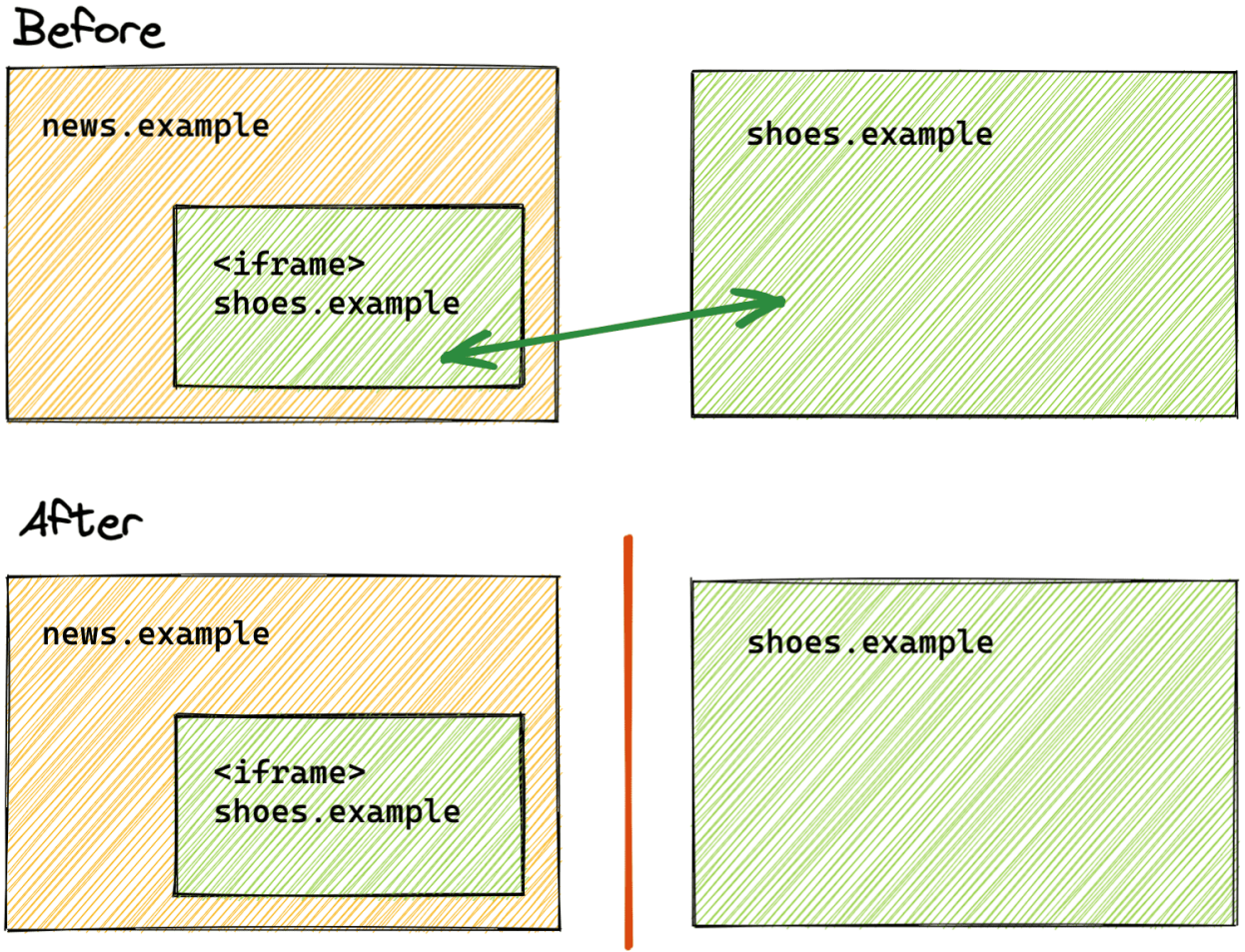
FENCED FRAMES

Позволява вграждане на съдържание от трета страна, без cross-site споделяне на данни.

<fencedframe> е HTML елемент подобен на iframe, но прилагащ специфични ограничения върху комуникацията между него и вграждащия го контекст.

В комбинация със storage partitioning, инициативат аще позволи максимално разделяне на данните и избягване на cross-domain проследяване.

Отново се прилагат изключения за специфични бизнес казуси, които позволява cross-site обмен на съдържание, напр. opaque-ads


Before
news.example
<iframe>
shoes.example
shoes.example
After
news.example
<iframe>
shoes.example
shoes.example

PRIVATE STATE TOKENS (ex-TRUST TOKENS)

Функционалност, предвидена да валидира cross-site самоличността на потребителите, чрез използване на криптографски токъни (вижте тук обмения им курс за деня).

Лимитира нуждата от пасивно проследяване, напр. чрез device fingerprinting, IP monitoring, промени в device state.

Важни напр. за идентифицирането на ботове, генериращи изкуствен трафик/кликове.

FEDERATED CREDENTIAL MANAGEMENT API

Предвидено е да обслужва нуждите на услуги, които реализират federated identity services. Пример за такива услуги са SSO доставчиците.

За да се ограничат възможностите за злоупотреба с текущите решения, се въвежда концепцията за доверена трета страна – Identity provider (IdP)

ДОПЪЛНИТЕЛНИ РЕСУРСИ

Private State Tokens (ex-Trust Tokens)

Topics API

Protected Audience API

Attribution Reporting

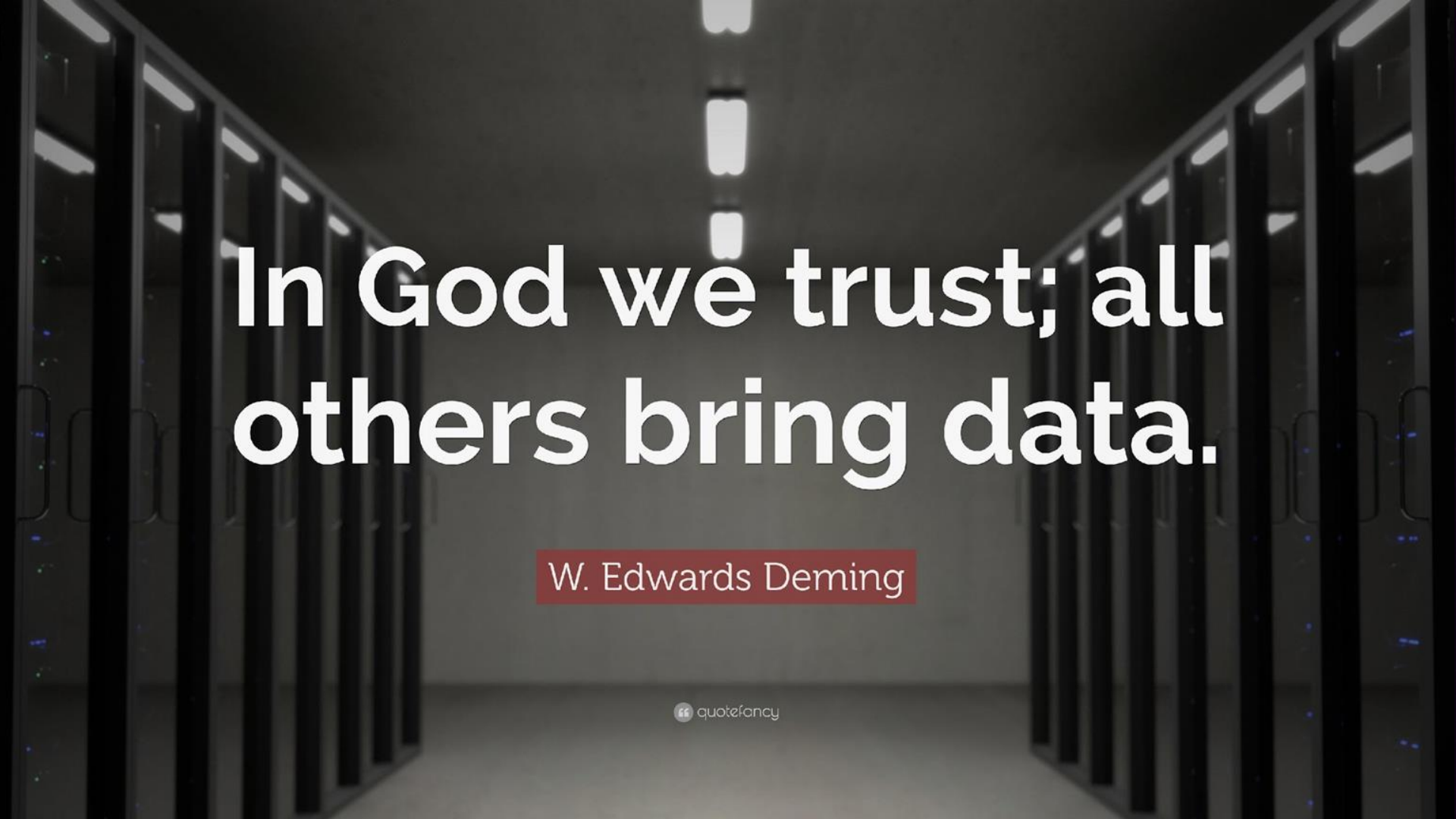
Related Website Sets

Shared Storage

Cookies Having Independent Partitioned State (CHIPS)

Fenced frames

Federated Credential Management API


In God we trust; all others bring data.
W. Edwards Deming
quotefancy

БЛАГОДАРЯ ЗА ВНИМАНИЕТО!