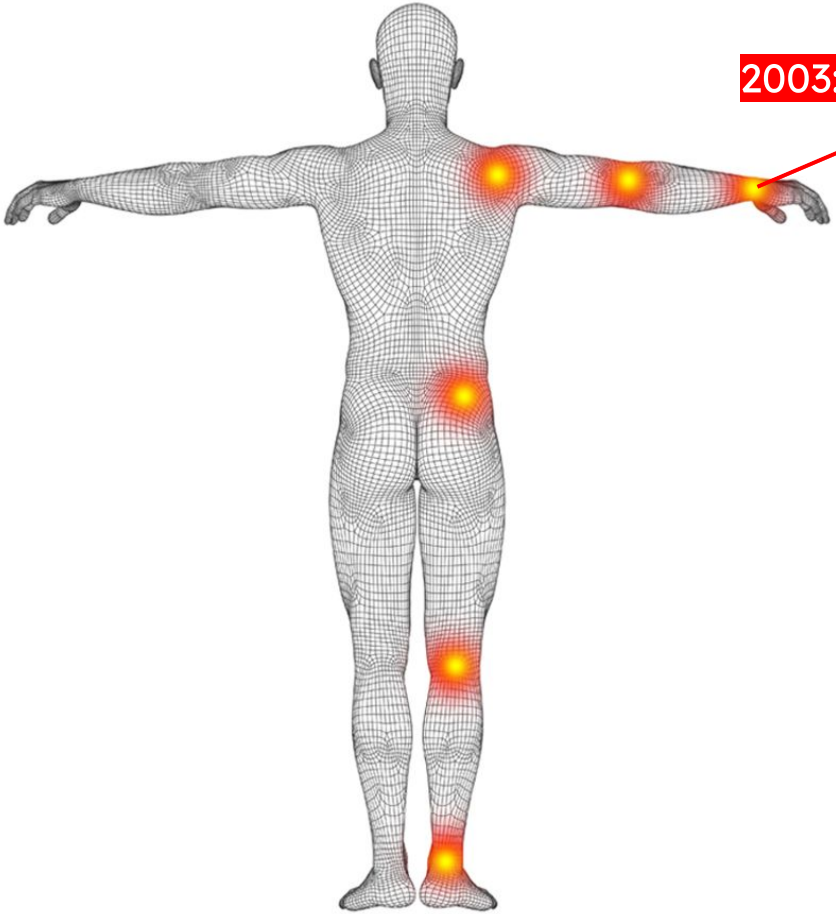
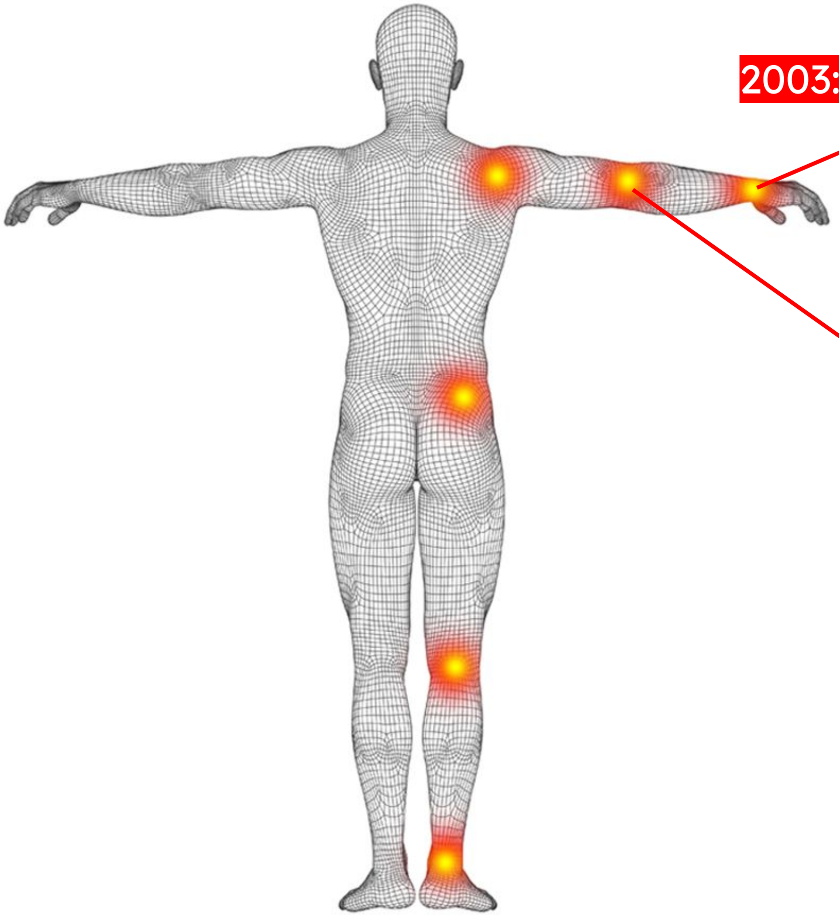
Out of the frying pan…
…into the **fire**

@SimoAhava from @Team_Simmer

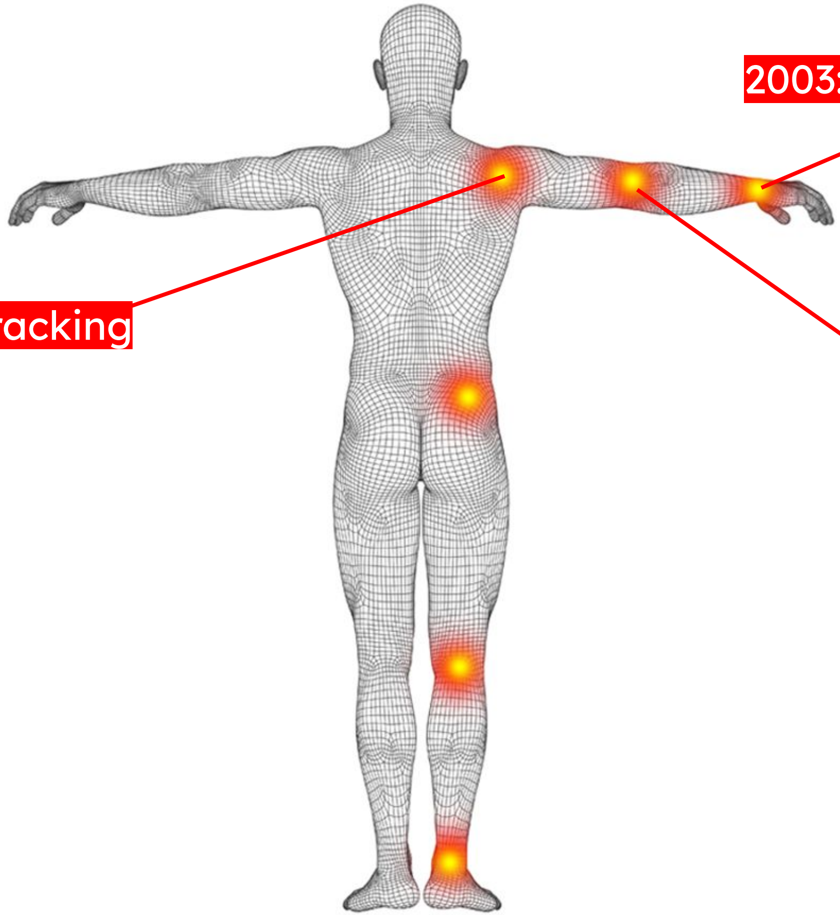


2003: Safari blocks 3P cookies



2003: Safari blocks 3P cookies

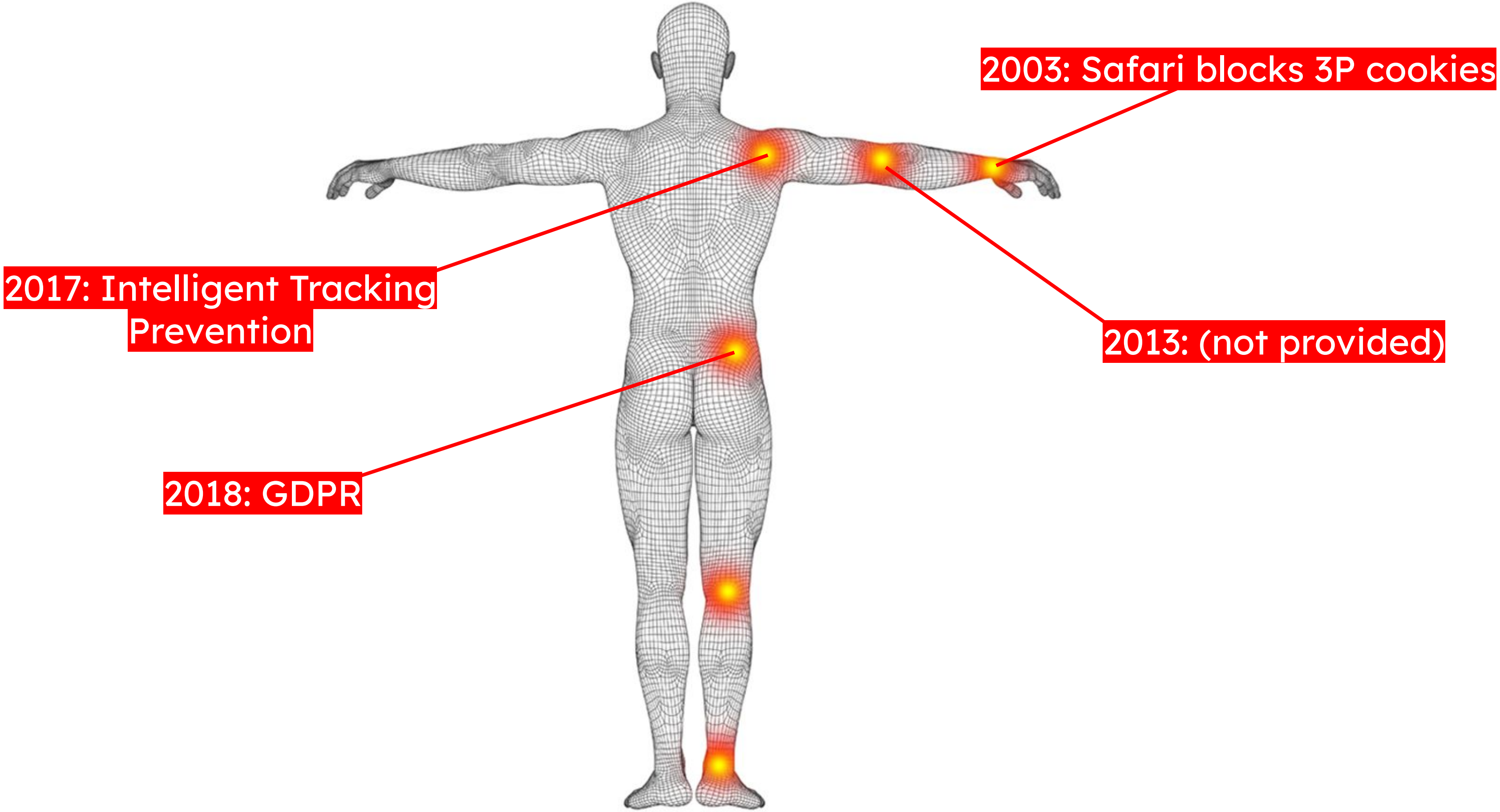
2013: (not provided)



2003: Safari blocks 3P cookies

2017: Intelligent Tracking Prevention

2013: (not provided)

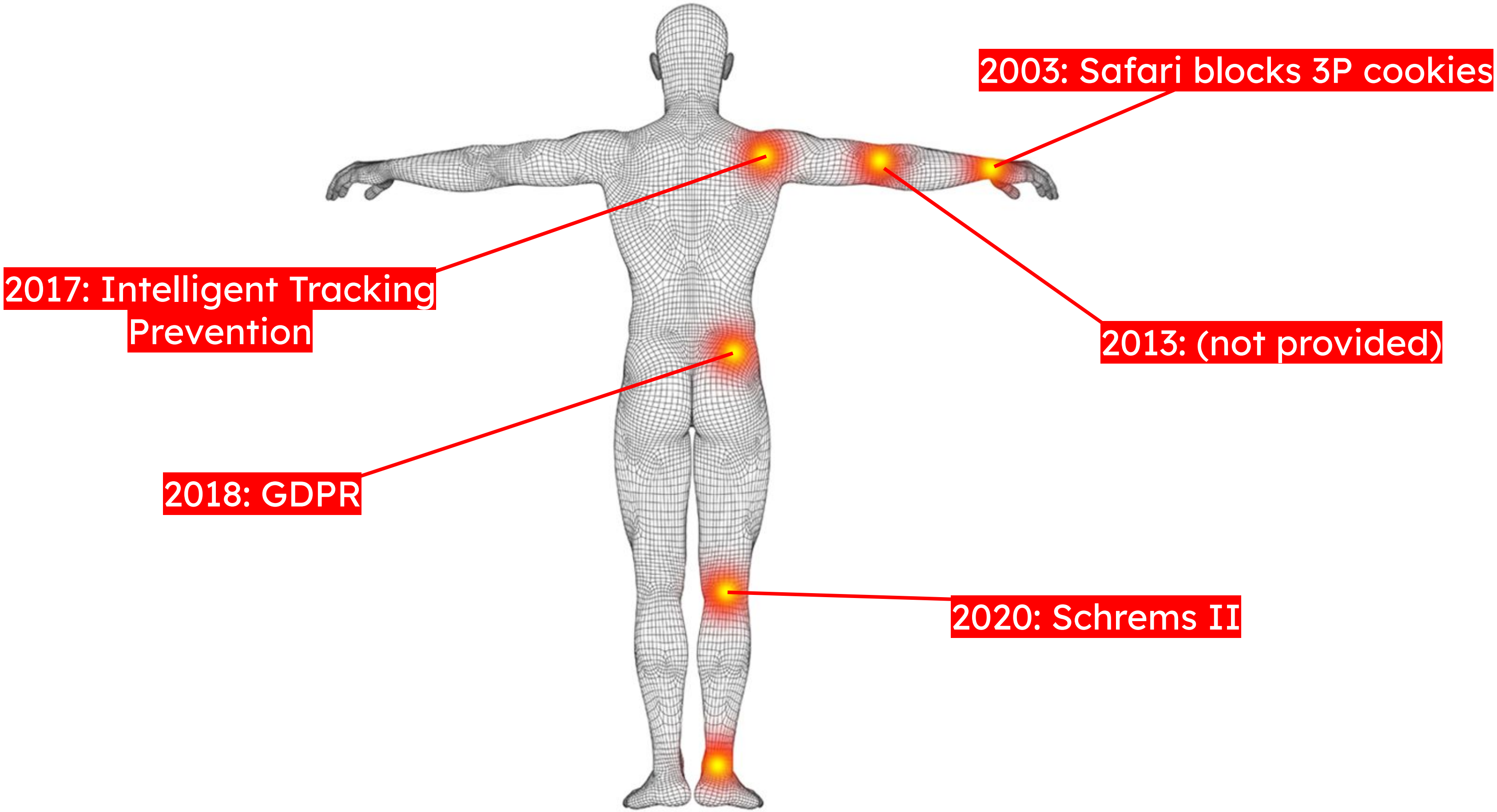


2003: Safari blocks 3P cookies

2017: Intelligent Tracking Prevention

2013: (not provided)

2018: GDPR



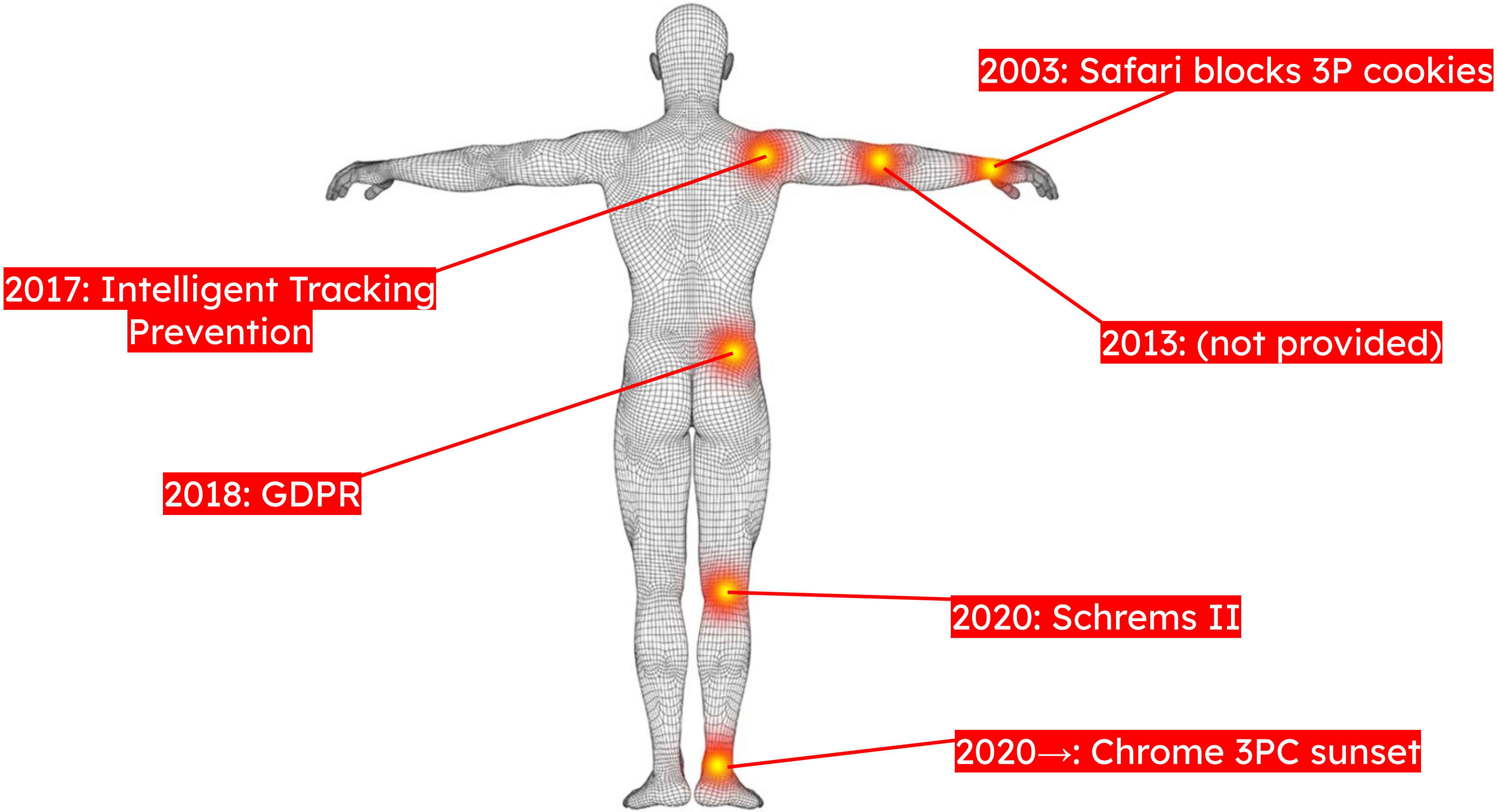
2003: Safari blocks 3P cookies

2017: Intelligent Tracking Prevention

2013: (not provided)

2018: GDPR

2020: Schrems II



2003: Safari blocks 3P cookies

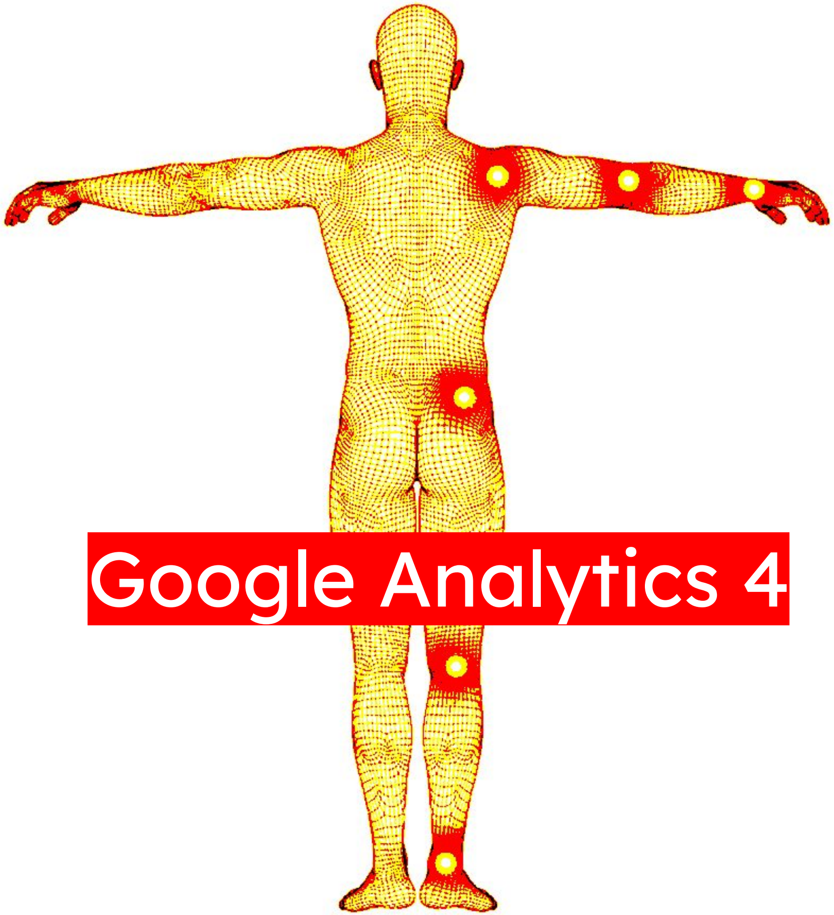
2017: Intelligent Tracking Prevention

2013: (not provided)

2018: GDPR

2020: Schrems II

2020→: Chrome 3PC sunset



Google Analytics 4

You should have stopped with the pain

2024 and onwards

I. Cookie expiration (WebKit)

II. Consent Mode (Google)

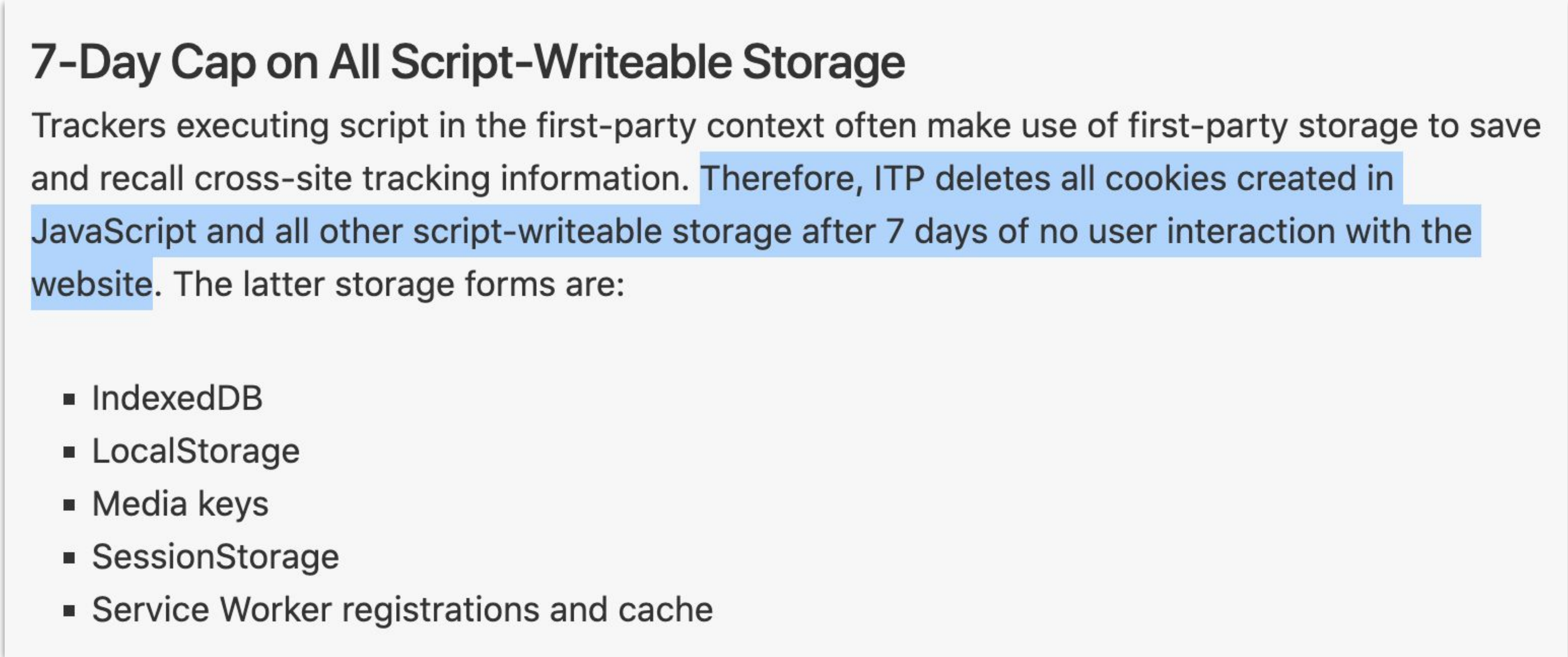
III. First-party data (AdTech)

IV. Server-side tagging (Google)

V. Analytics without GA4 (Piwik PRO, Amplitude, BigQuery…)

How dare they

Cookie expiration

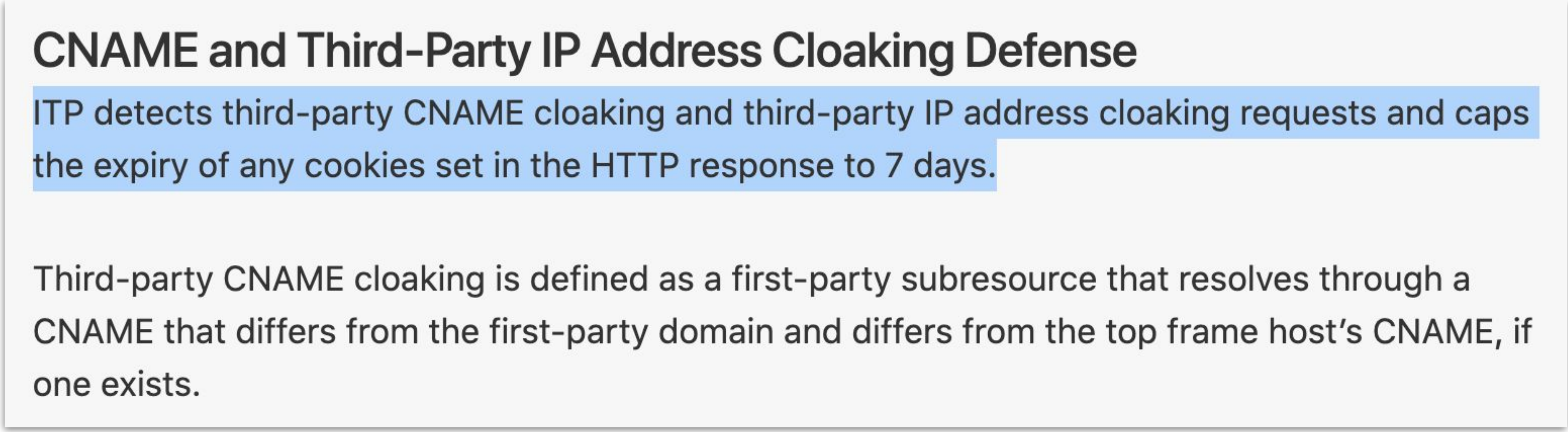


7-Day Cap on All Script-Writeable Storage

Trackers executing script in the first-party context often make use of first-party storage to save and recall cross-site tracking information. Therefore, ITP deletes all cookies created in JavaScript and all other script-writeable storage after 7 days of no user interaction with the website. The latter storage forms are:

- IndexedDB
- LocalStorage
- Media keys
- SessionStorage
- Service Worker registrations and cache

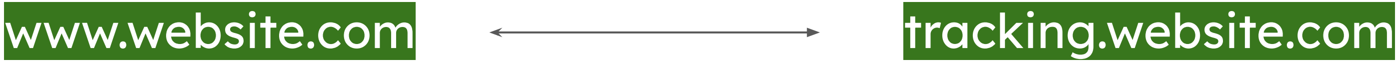
https://webkit.org/tracking-prevention/

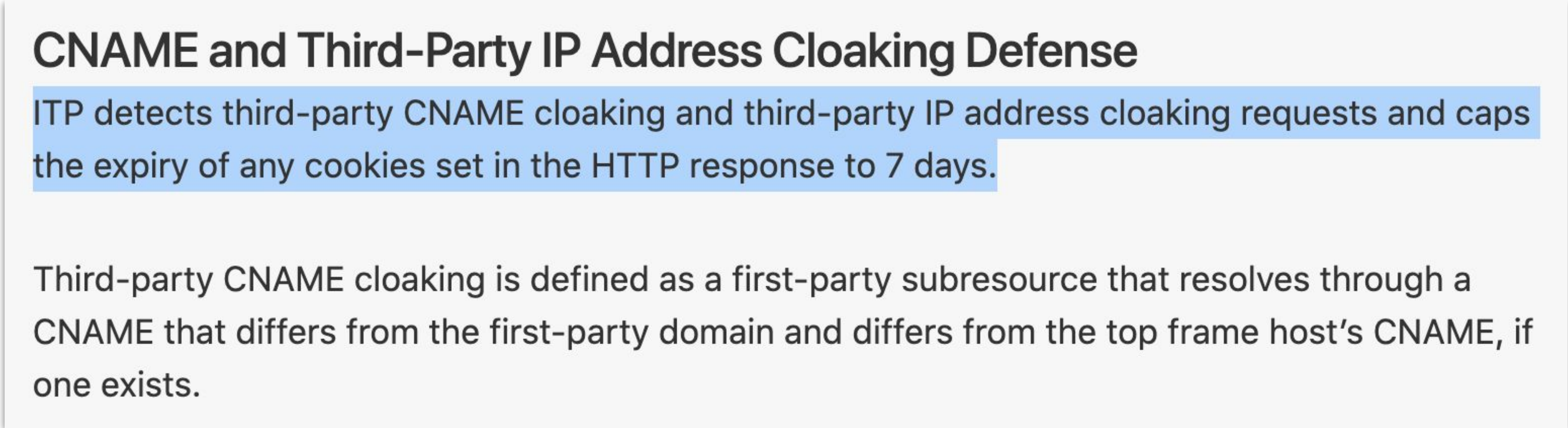


CNAME and Third-Party IP Address Cloaking Defense

ITP detects third-party CNAME cloaking and third-party IP address cloaking requests and caps the expiry of any cookies set in the HTTP response to 7 days.

Third-party CNAME cloaking is defined as a first-party subresource that resolves through a CNAME that differs from the first-party domain and differs from the top frame host's CNAME, if one exists.

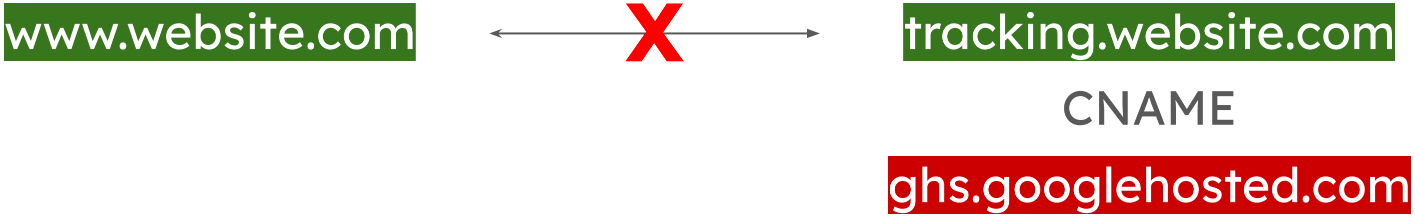




CNAME and Third-Party IP Address Cloaking Defense

ITP detects third-party CNAME cloaking and third-party IP address cloaking requests and caps the expiry of any cookies set in the HTTP response to 7 days.

Third-party CNAME cloaking is defined as a first-party subresource that resolves through a CNAME that differs from the first-party domain and differs from the top frame host’s CNAME, if one exists.

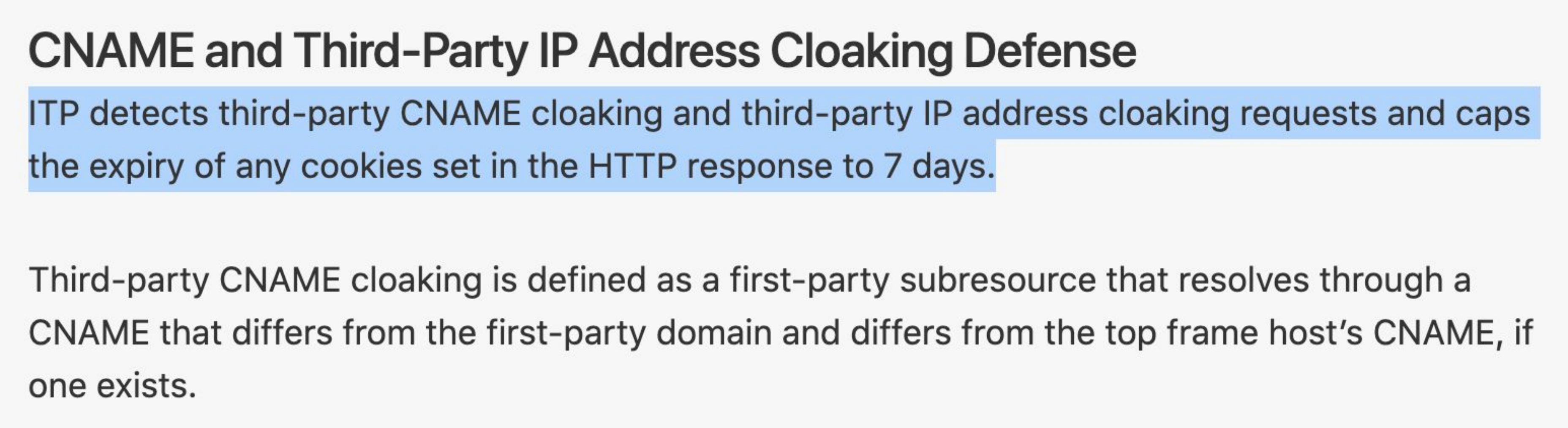


www.website.com

tracking.website.com

CNAME

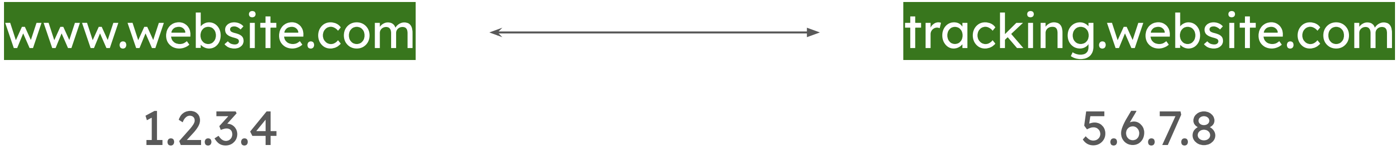
ghs.googlehosted.com



CNAME and Third-Party IP Address Cloaking Defense

ITP detects third-party CNAME cloaking and third-party IP address cloaking requests and caps the expiry of any cookies set in the HTTP response to 7 days.

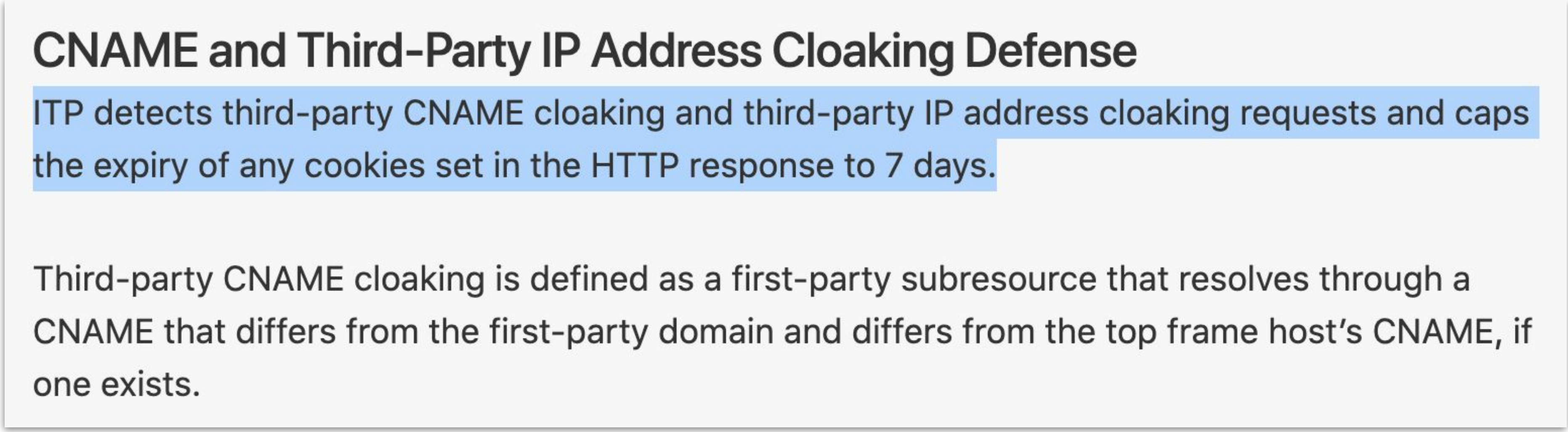
Third-party CNAME cloaking is defined as a first-party subresource that resolves through a CNAME that differs from the first-party domain and differs from the top frame host's CNAME, if one exists.



www.website.com ↔ tracking.website.com

1.2.3.4

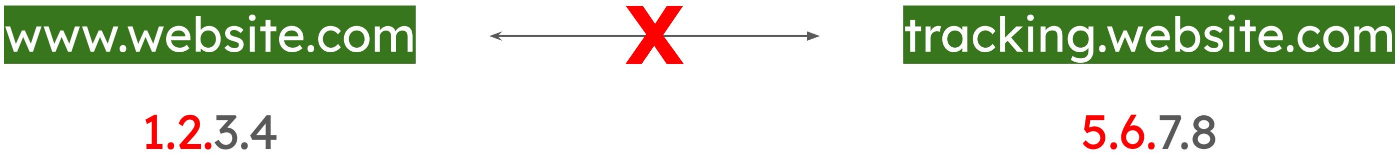
5.6.7.8



CNAME and Third-Party IP Address Cloaking Defense

ITP detects third-party CNAME cloaking and third-party IP address cloaking requests and caps the expiry of any cookies set in the HTTP response to 7 days.

Third-party CNAME cloaking is defined as a first-party subresource that resolves through a CNAME that differs from the first-party domain and differs from the top frame host’s CNAME, if one exists.

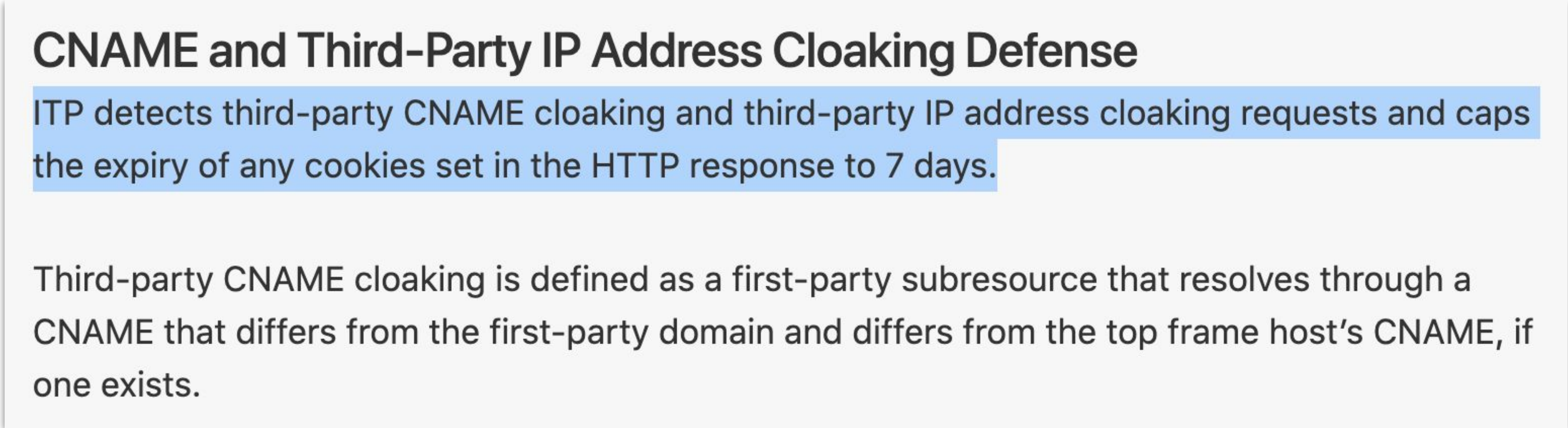


www.website.com

1.2.3.4

tracking.website.com

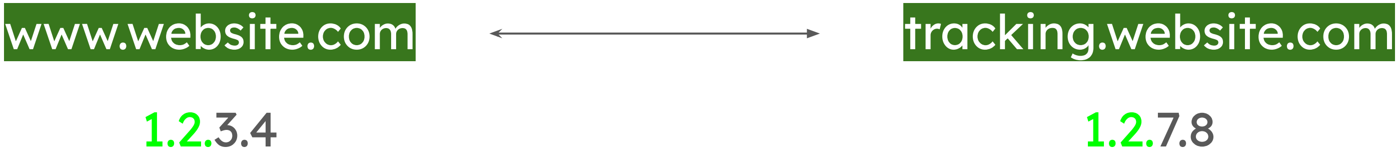
5.6.7.8



CNAME and Third-Party IP Address Cloaking Defense

ITP detects third-party CNAME cloaking and third-party IP address cloaking requests and caps the expiry of any cookies set in the HTTP response to 7 days.

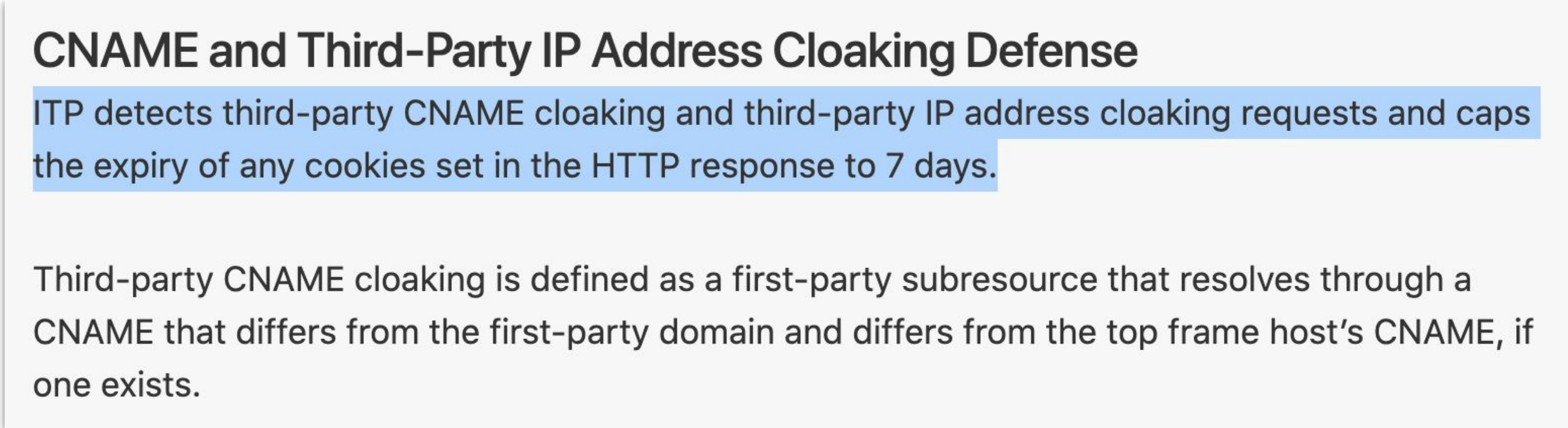
Third-party CNAME cloaking is defined as a first-party subresource that resolves through a CNAME that differs from the first-party domain and differs from the top frame host’s CNAME, if one exists.



www.website.com ↔ tracking.website.com

1.2.3.4

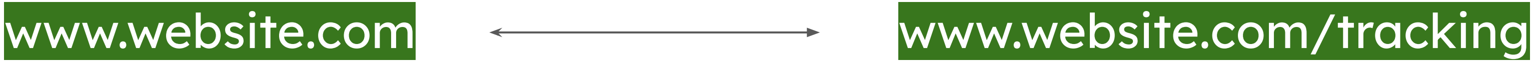
1.2.7.8



CNAME and Third-Party IP Address Cloaking Defense

ITP detects third-party CNAME cloaking and third-party IP address cloaking requests and caps the expiry of any cookies set in the HTTP response to 7 days.

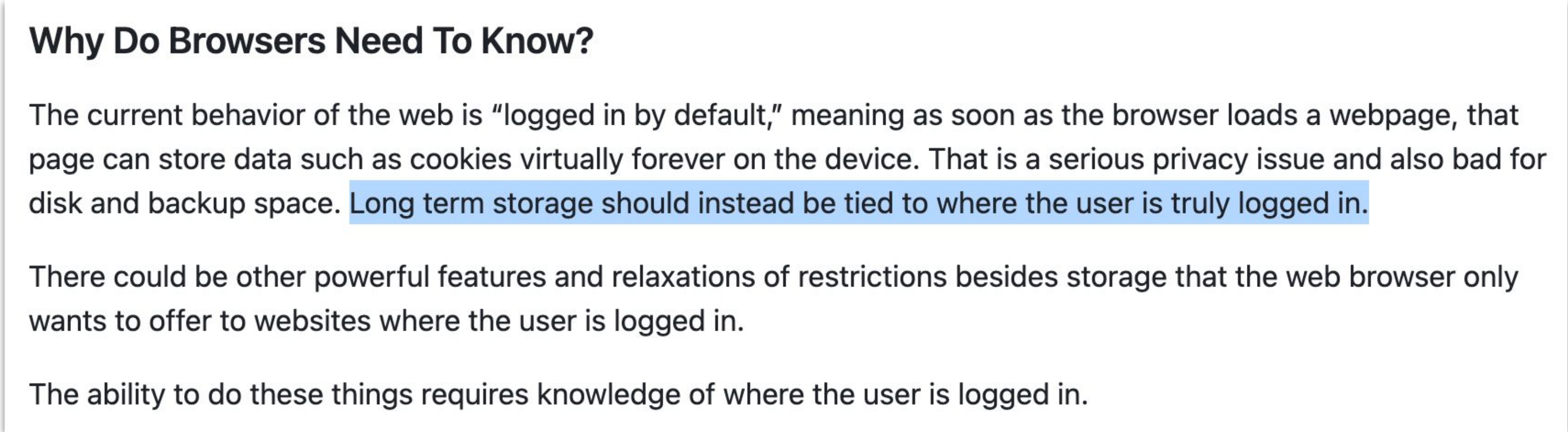
Third-party CNAME cloaking is defined as a first-party subresource that resolves through a CNAME that differs from the first-party domain and differs from the top frame host's CNAME, if one exists.



www.website.com

www.website.com/tracking

WebKit has yet to reveal its deadliest feature…



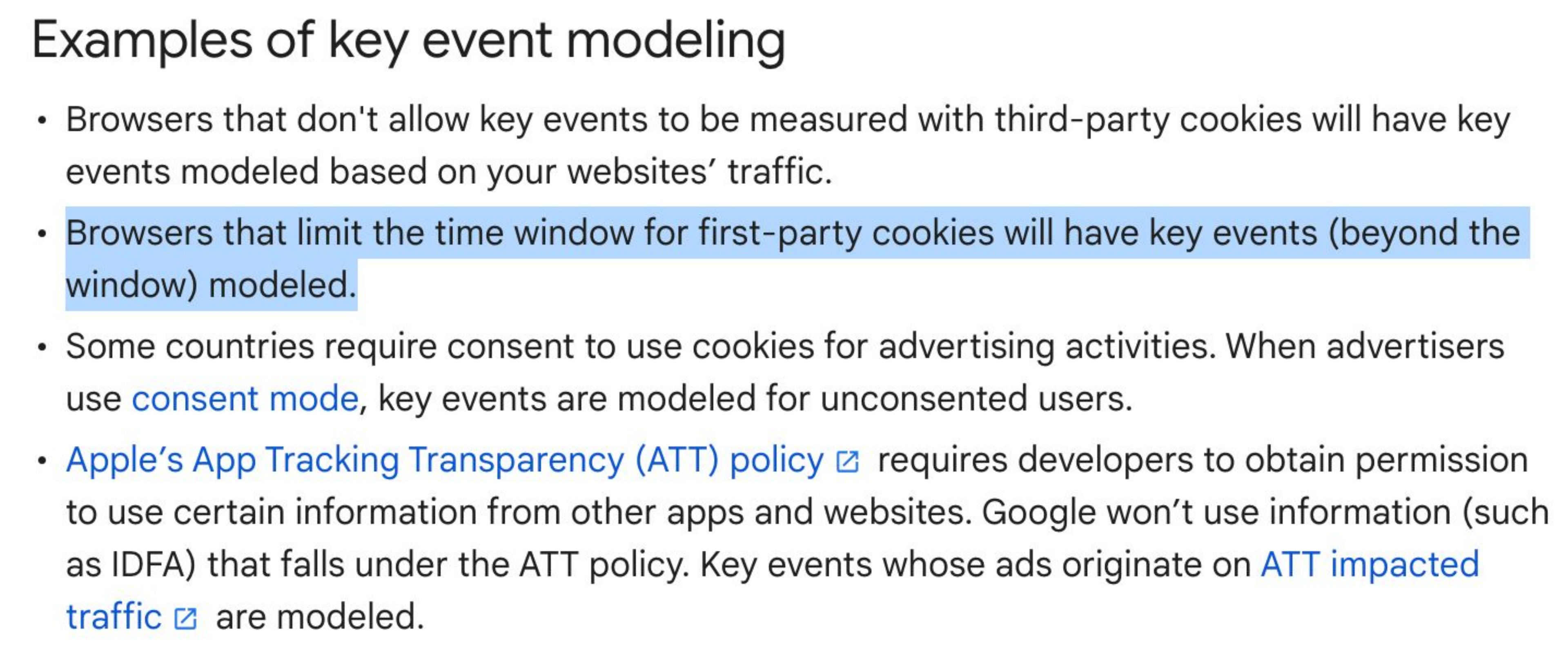
Why Do Browsers Need To Know?

The current behavior of the web is “logged in by default,” meaning as soon as the browser loads a webpage, that page can store data such as cookies virtually forever on the device. That is a serious privacy issue and also bad for disk and backup space. Long term storage should instead be tied to where the user is truly logged in.

There could be other powerful features and relaxations of restrictions besides storage that the web browser only wants to offer to websites where the user is logged in.

The ability to do these things requires knowledge of where the user is logged in.

https://github.com/privacycg/is-logged-in



Examples of key event modeling

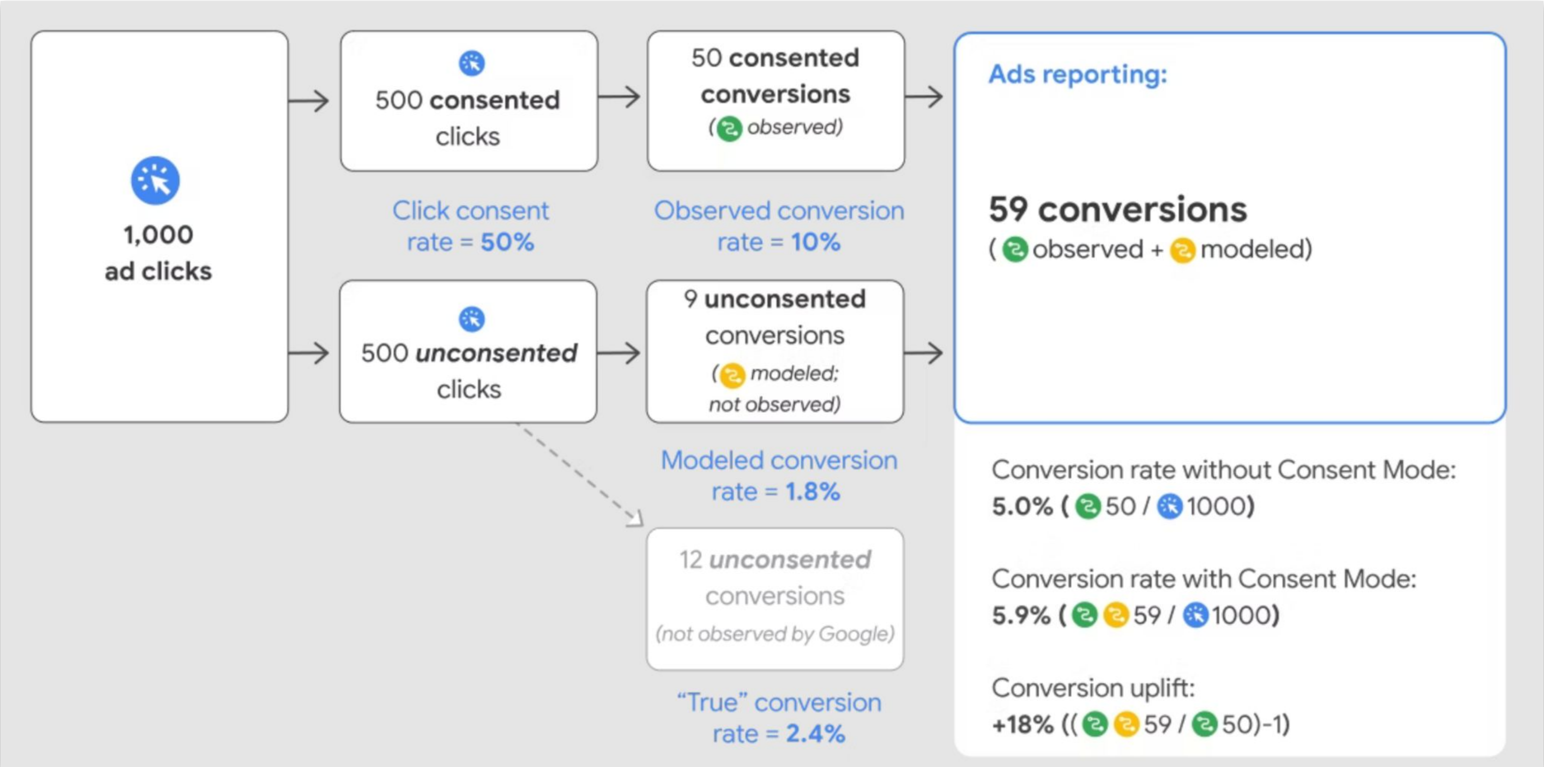
- Browsers that don't allow key events to be measured with third-party cookies will have key events modeled based on your websites' traffic.
- Browsers that limit the time window for first-party cookies will have key events (beyond the window) modeled.
- Some countries require consent to use cookies for advertising activities. When advertisers use consent mode, key events are modeled for unconsented users.
- Apple's App Tracking Transparency (ATT) policy requires developers to obtain permission to use certain information from other apps and websites. Google won't use information (such as IDFA) that falls under the ATT policy. Key events whose ads originate on ATT impacted traffic are modeled.

https://support.google.com/analytics/answer/10710245?hl=en

WebKit has far more resources available for making sure that cross-site tracking dies than what you have available for circumventing its tracking prevention policies.

More lipstick on a pig

Consent Mode



🔵 1,000 ad clicks

🔵 500 **consented** clicks

Click consent rate = **50%**

50 **consented conversions** (🟢 *observed)*

Observed conversion rate = **10%**

🔵 500 ***unconsented*** clicks

9 **unconsented** conversions (🟡 *modeled; not observed)*

Modeled conversion rate = **1.8%**

12 ***unconsented*** conversions *(not observed by Google)*

"True" conversion rate = **2.4%**

Ads reporting:

59 conversions

(🟢 observed + 🟡 modeled)

Conversion rate without Consent Mode:
5.0% (🟢 50 / 🔵 1000**)**

Conversion rate with Consent Mode:
5.9% (🟢 🟡 59 / 🔵 1000**)**

Conversion uplift:
+18% ((🟢 🟡 59 / 🟢 50)-1)

Source: Google webinar

BASIC Consent Mode:

1. Consent Default: All denied
2. Consent Update
3. Tags that use granted storage fire

ADVANCED Consent Mode:

1. Consent Default: All denied
2. Tags fire
3. Consent Update

BASIC Consent Mode:

1. Consent Default: All denied
2. Consent Update
3. Tags that use granted storage fire

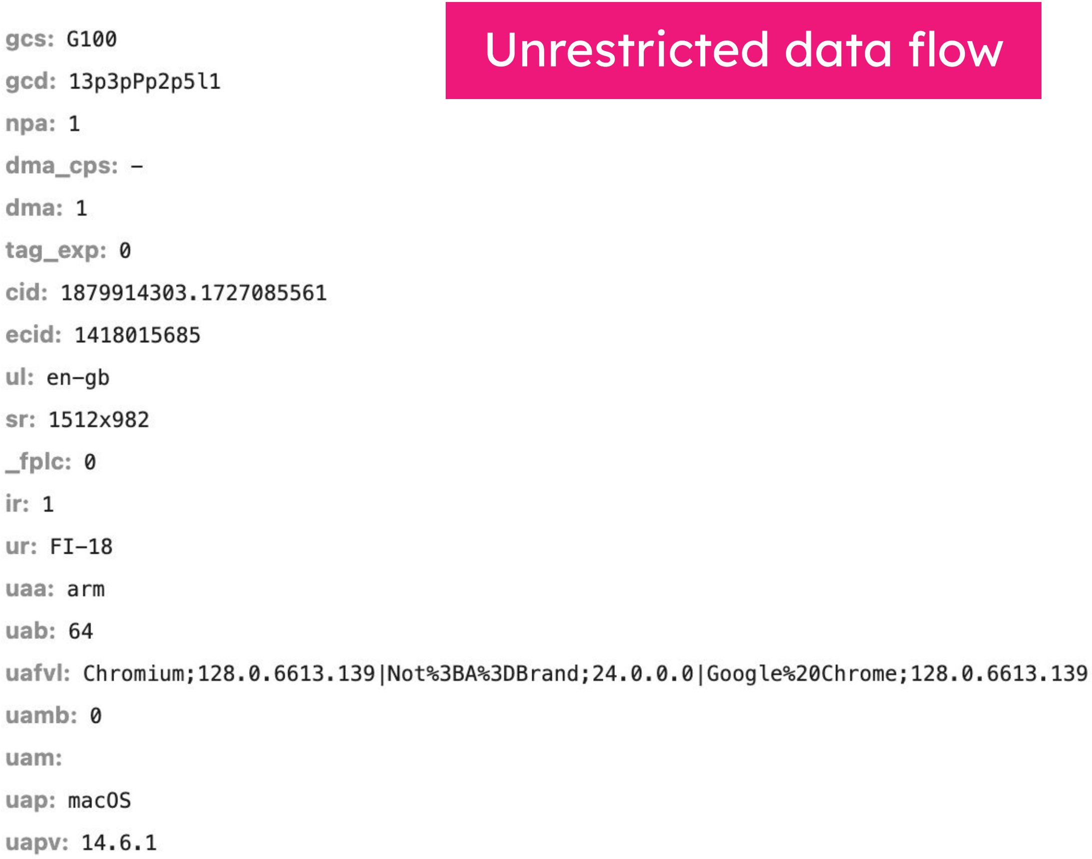
Only consent granted data
No behavioral modeling
Limited conversion modeling

ADVANCED Consent Mode:

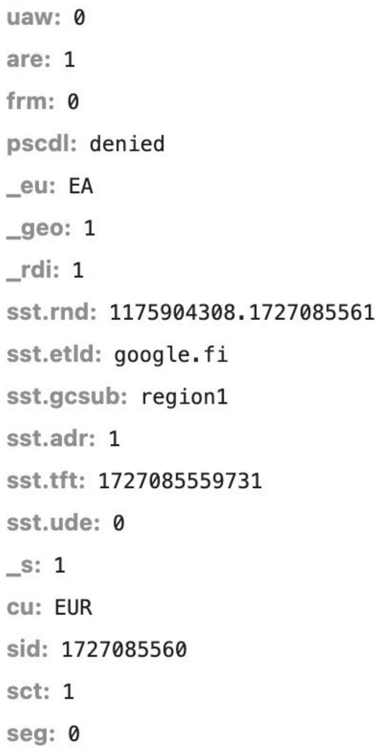
1. Consent Default: All denied
2. Tags fire
3. Consent Update

Unrestricted data flow
GDPR / ePD?
Full modeling capabilities

Unrestricted data flow

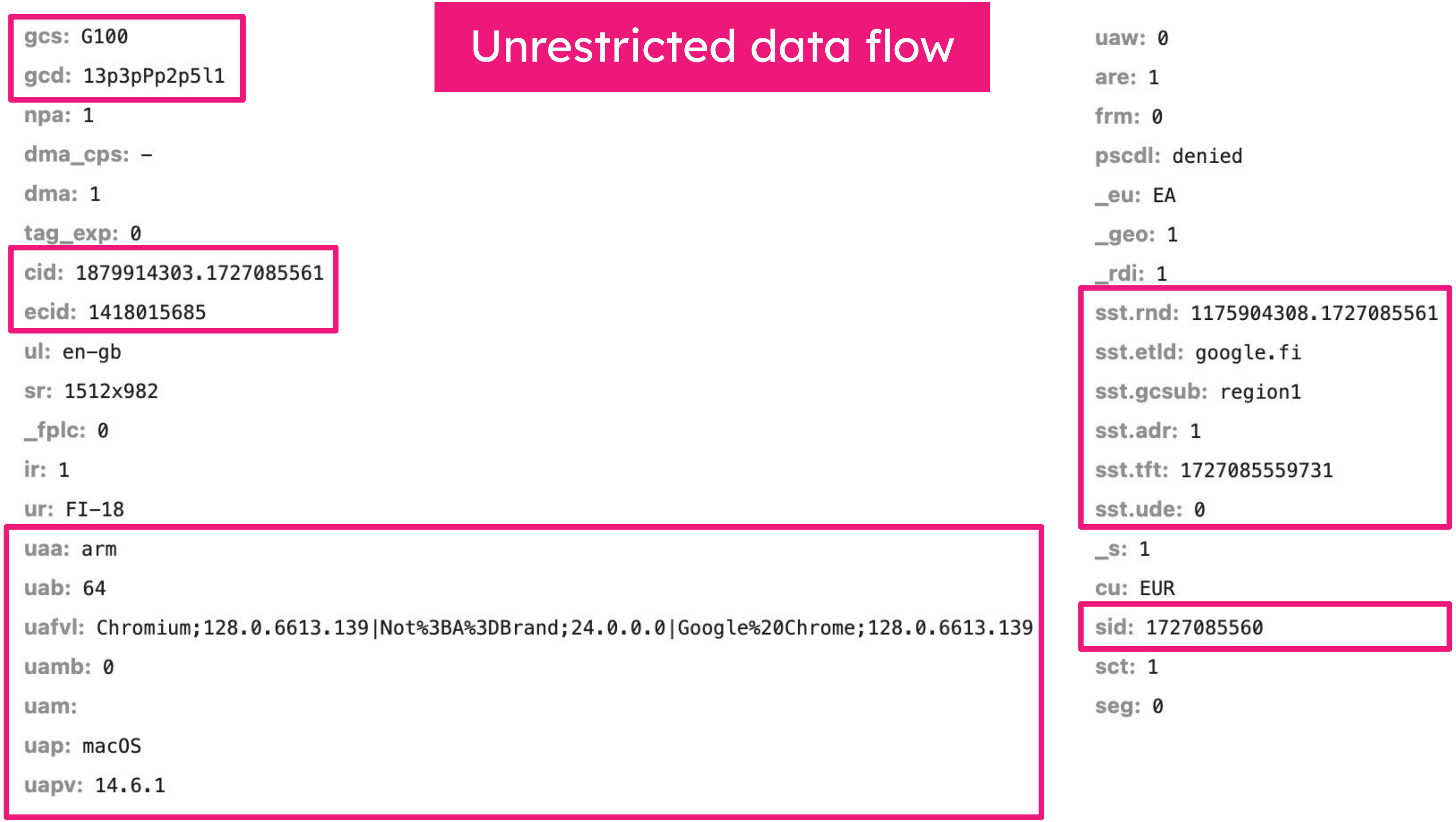


```
gcs: G100
gcd: 13p3pPp2p5l1
npa: 1
dma_cps: -
dma: 1
tag_exp: 0
cid: 1879914303.1727085561
ecid: 1418015685
ul: en-gb
sr: 1512x982
_fplc: 0
ir: 1
ur: FI-18
uaa: arm
uab: 64
uafvl: Chromium;128.0.6613.139|Not%3BA%3DBrand;24.0.0.0|Google%20Chrome;128.0.6613.139
uamb: 0
uam:
uap: macOS
uapv: 14.6.1
```



```
uaw: 0
are: 1
frm: 0
pscdl: denied
_eu: EA
_geo: 1
_rdi: 1
sst.rnd: 1175904308.1727085561
sst.etld: google.fi
sst.gcsub: region1
sst.adr: 1
sst.tft: 1727085559731
sst.ude: 0
_s: 1
cu: EUR
sid: 1727085560
sct: 1
seg: 0
```

Unrestricted data flow



```
gcs: G100
gcd: 13p3pPp2p5l1
npa: 1
dma_cps: -
dma: 1
tag_exp: 0
cid: 1879914303.1727085561
ecid: 1418015685
ul: en-gb
sr: 1512x982
_fplc: 0
ir: 1
ur: FI-18
uaa: arm
uab: 64
uafvl: Chromium;128.0.6613.139|Not%3BA%3DBrand;24.0.0.0|Google%20Chrome;128.0.6613.139
uamb: 0
uam:
uap: macOS
uapv: 14.6.1
```

```
uaw: 0
are: 1
frm: 0
pscdl: denied
_eu: EA
_geo: 1
_rdi: 1
sst.rnd: 1175904308.1727085561
sst.etld: google.fi
sst.gcsub: region1
sst.adr: 1
sst.tft: 1727085559731
sst.ude: 0
_s: 1
cu: EUR
sid: 1727085560
sct: 1
seg: 0
```

Why do “anonymous” pings permit…

User Agent / Client Hints

User ID

Geolocation

Transaction ID

Event Parameters

User Properties

Advanced Consent Mode

Pros	Cons
Passes the Simo-test	
Does what it promises regarding storage access	
The model hides the individual	
Raw data is exported to BQ	

Advanced Consent Mode

Pros	Cons
Passes the Simo-test	Collects far more than is probably necessary
Does what it promises regarding storage access	Questionable regarding GDPR
The model hides the individual	The model is a black box
Raw data is exported to BQ	Raw data is exported to BQ
	The optics are not good
	Non-zero risk
	The fox guards the hen house

In what context is it OK to first ask for consent, and upon denial, continue tracking anyway *without* a minimal data footprint?

Help the poor ad tech vendors

First-party data

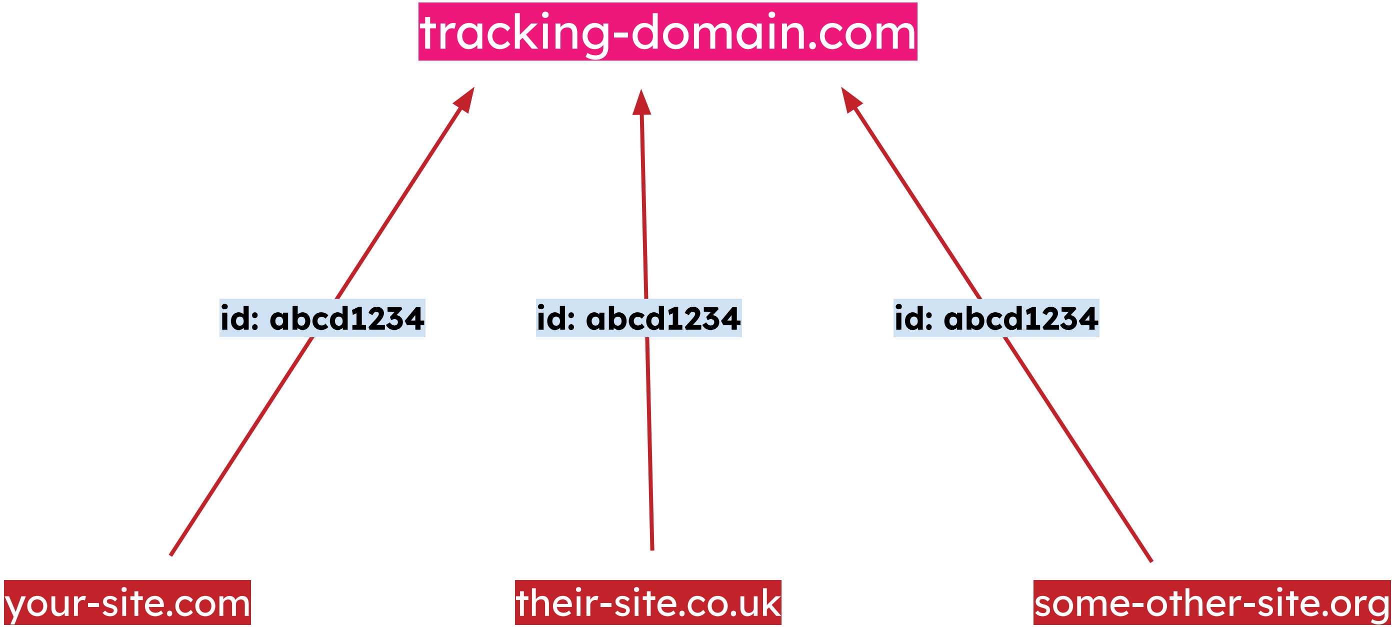
tracking-domain.com

your-site.com

their-site.co.uk

some-other-site.org

Cross-site tracking with 3P cookies



tracking-domain.com

id: abcd1234

id: abcd1234

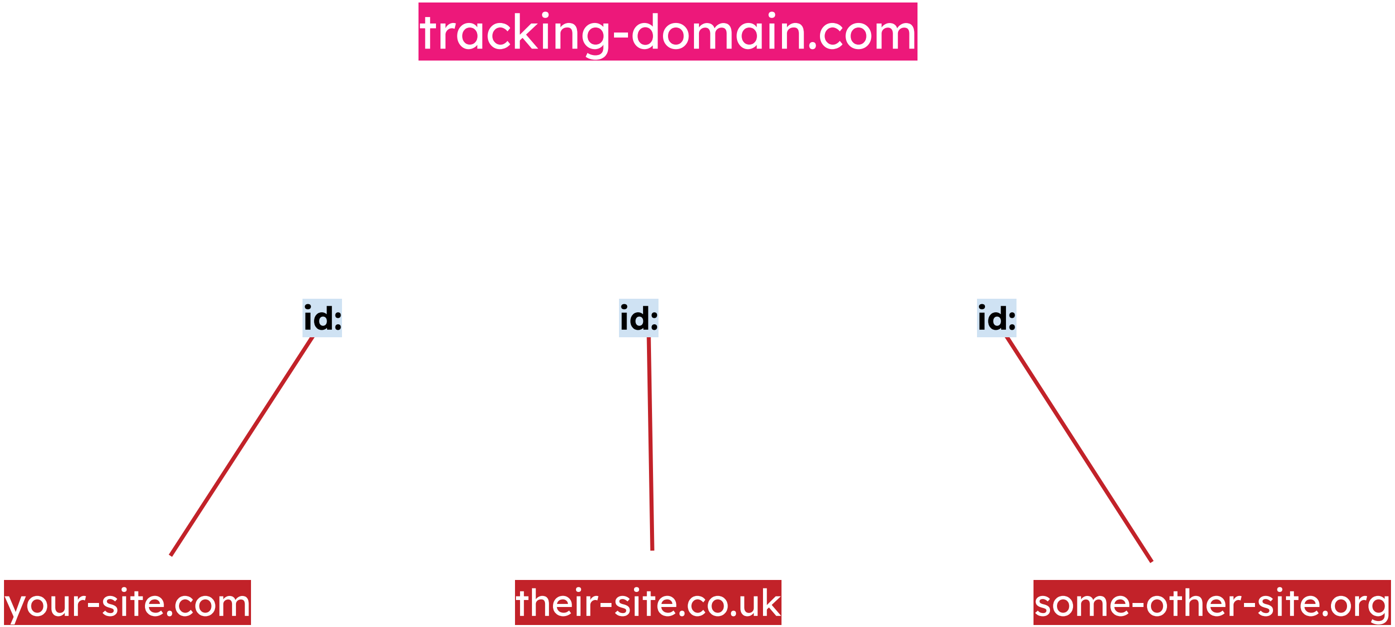
id: abcd1234

your-site.com

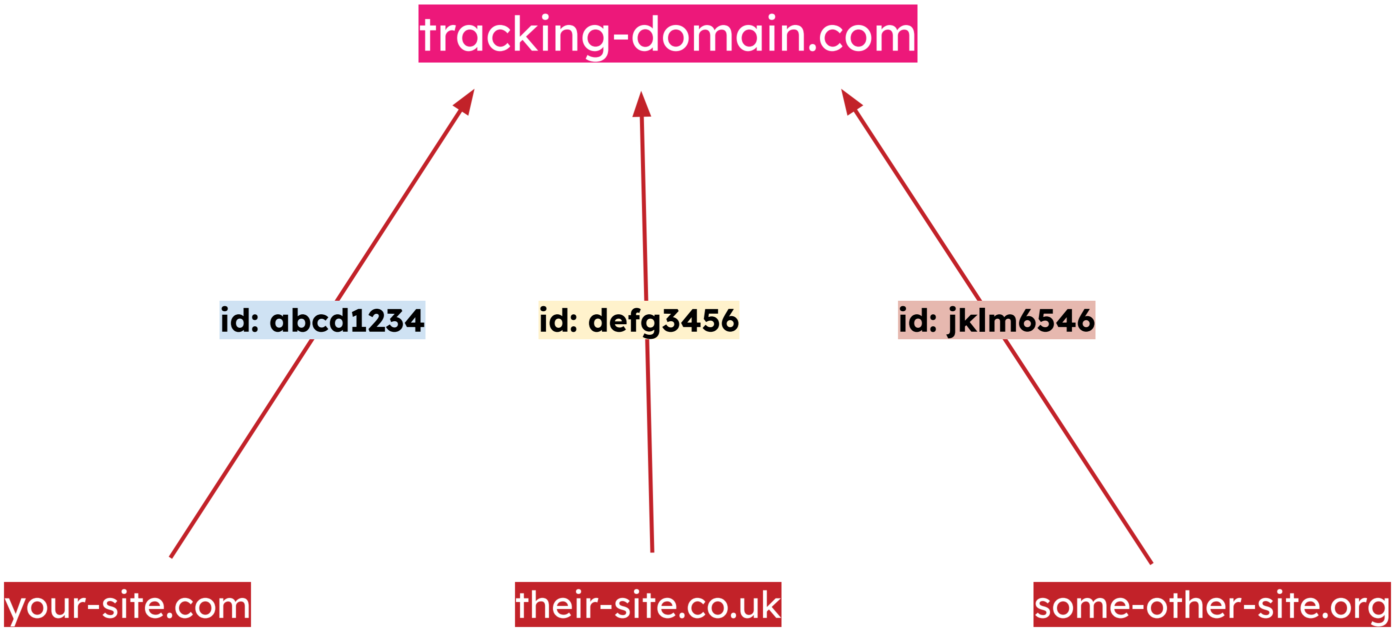
their-site.co.uk

some-other-site.org

3P cookies blocked



3P cookies partitioned



tracking-domain.com

id: abcd1234

id: defg3456

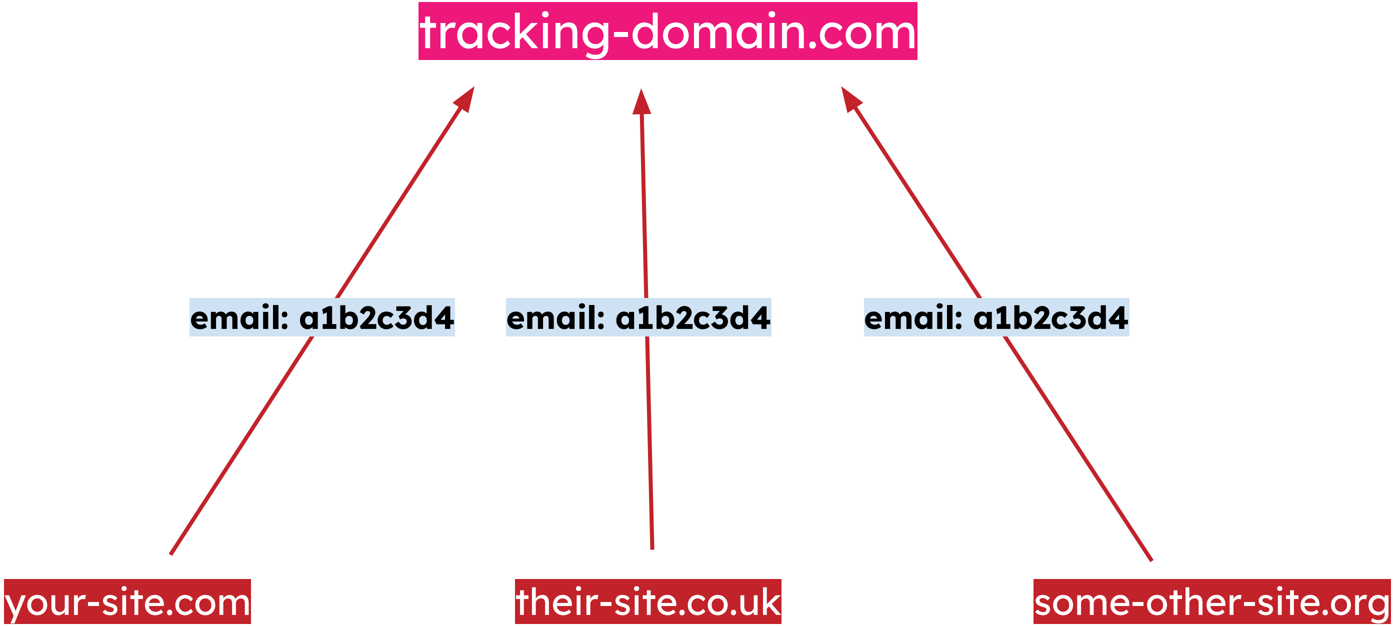
id: jklm6546

your-site.com

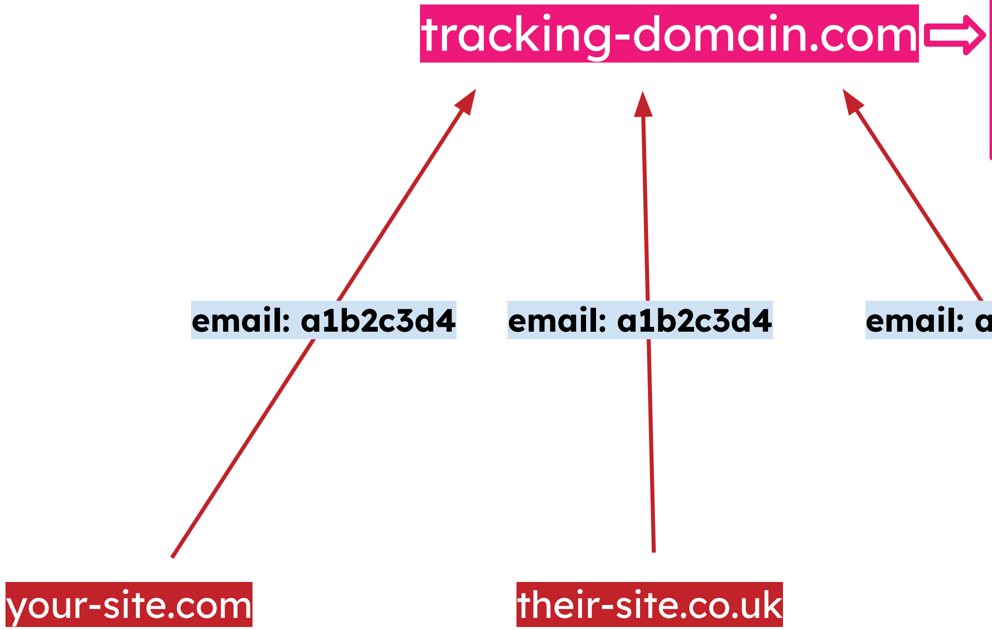
their-site.co.uk

some-other-site.org

Cross-site tracking with first-party data



Cross-site tracking with first-party data



tracking-domain.com

email: a1b2c3d4

email: a1b2c3d4

email: a1b2c3d4

your-site.com

their-site.co.uk

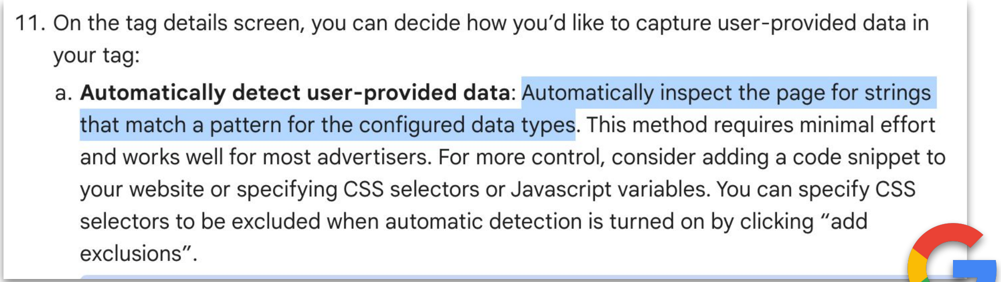
some-other-site.org

Email	Hash
...	...
...	...
simo@simo.com	a1b2c3d4
...	...
...	...

Hashing is for security, not for privacy

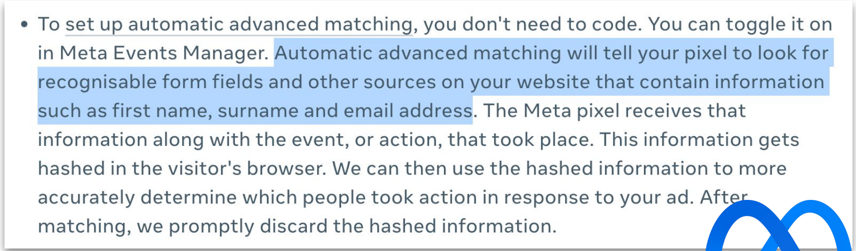
It protects data at transit and at storage, but it isn’t strictly an anonymization measure

Unlike 3P cookies, 1P data is valuable for all parties downstream – far greater risk of data leak/breach than with cookie identifiers

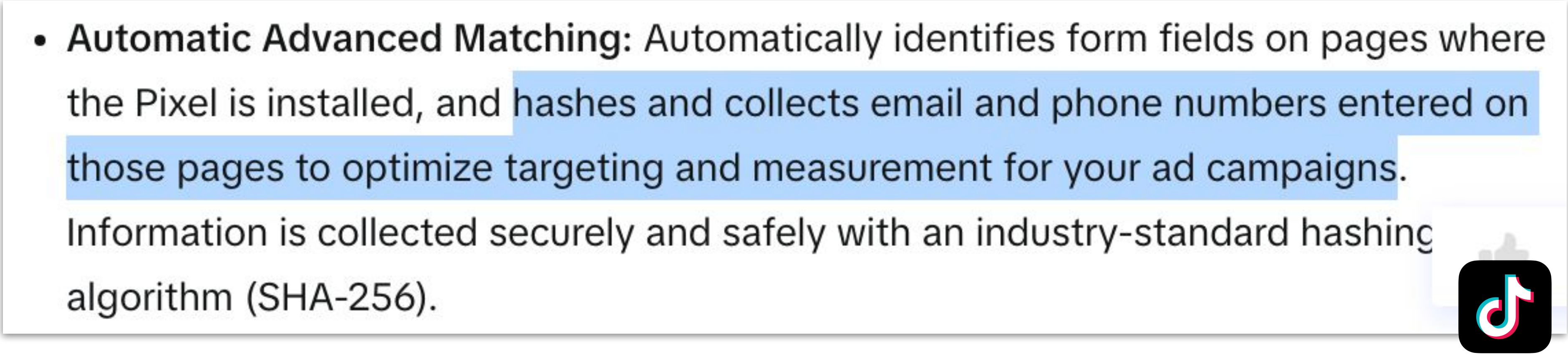


11. On the tag details screen, you can decide how you'd like to capture user-provided data in your tag:

    a. **Automatically detect user-provided data**: Automatically inspect the page for strings that match a pattern for the configured data types. This method requires minimal effort and works well for most advertisers. For more control, consider adding a code snippet to your website or specifying CSS selectors or Javascript variables. You can specify CSS selectors to be excluded when automatic detection is turned on by clicking "add exclusions".



- To set up automatic advanced matching, you don't need to code. You can toggle it on in Meta Events Manager. Automatic advanced matching will tell your pixel to look for recognisable form fields and other sources on your website that contain information such as first name, surname and email address. The Meta pixel receives that information along with the event, or action, that took place. This information gets hashed in the visitor's browser. We can then use the hashed information to more accurately determine which people took action in response to your ad. After matching, we promptly discard the hashed information.

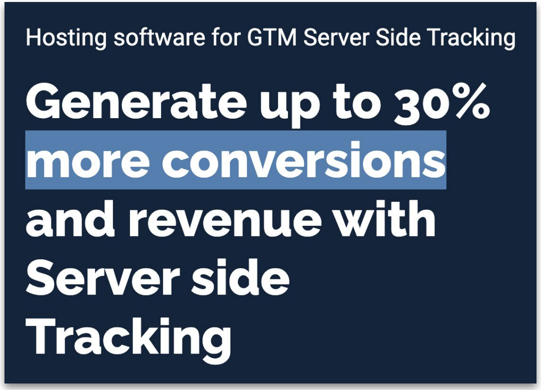


- **Automatic Advanced Matching:** Automatically identifies form fields on pages where the Pixel is installed, and hashes and collects email and phone numbers entered on those pages to optimize targeting and measurement for your ad campaigns. Information is collected securely and safely with an industry-standard hashing algorithm (SHA-256).

First-party data relies on hashed personal data that can be linked to decades of browsing behavior. It demands more scrutiny than cookie identifiers.

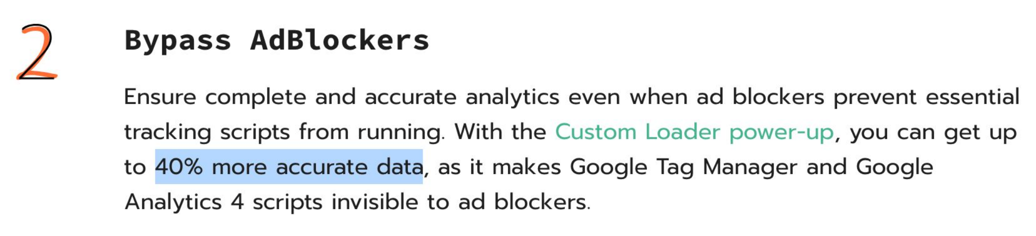
The curse of MORE DATA

Server-side tagging



Hosting software for GTM Server Side Tracking

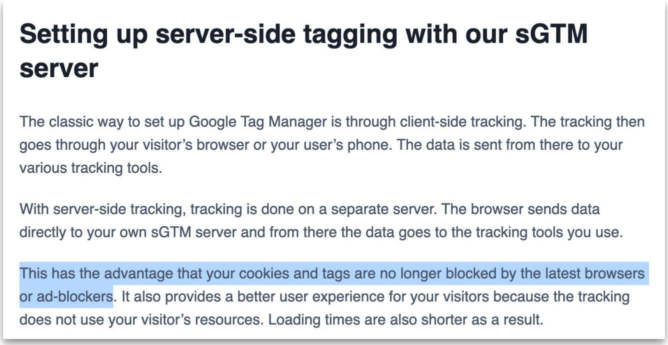
Generate up to 30% more conversions and revenue with Server side Tracking



2

Bypass AdBlockers

Ensure complete and accurate analytics even when ad blockers prevent essential tracking scripts from running. With the Custom Loader power-up, you can get up to 40% more accurate data, as it makes Google Tag Manager and Google Analytics 4 scripts invisible to ad blockers.

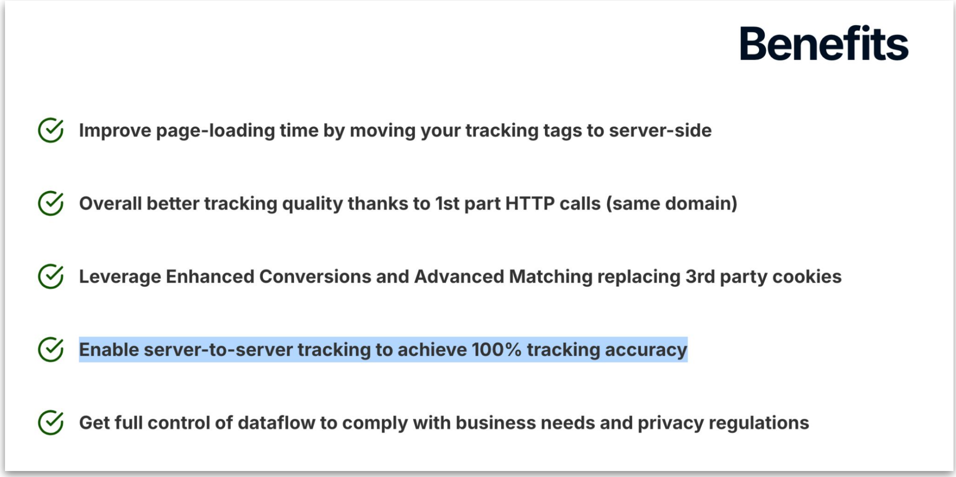


Setting up server-side tagging with our sGTM server

The classic way to set up Google Tag Manager is through client-side tracking. The tracking then goes through your visitor's browser or your user's phone. The data is sent from there to your various tracking tools.

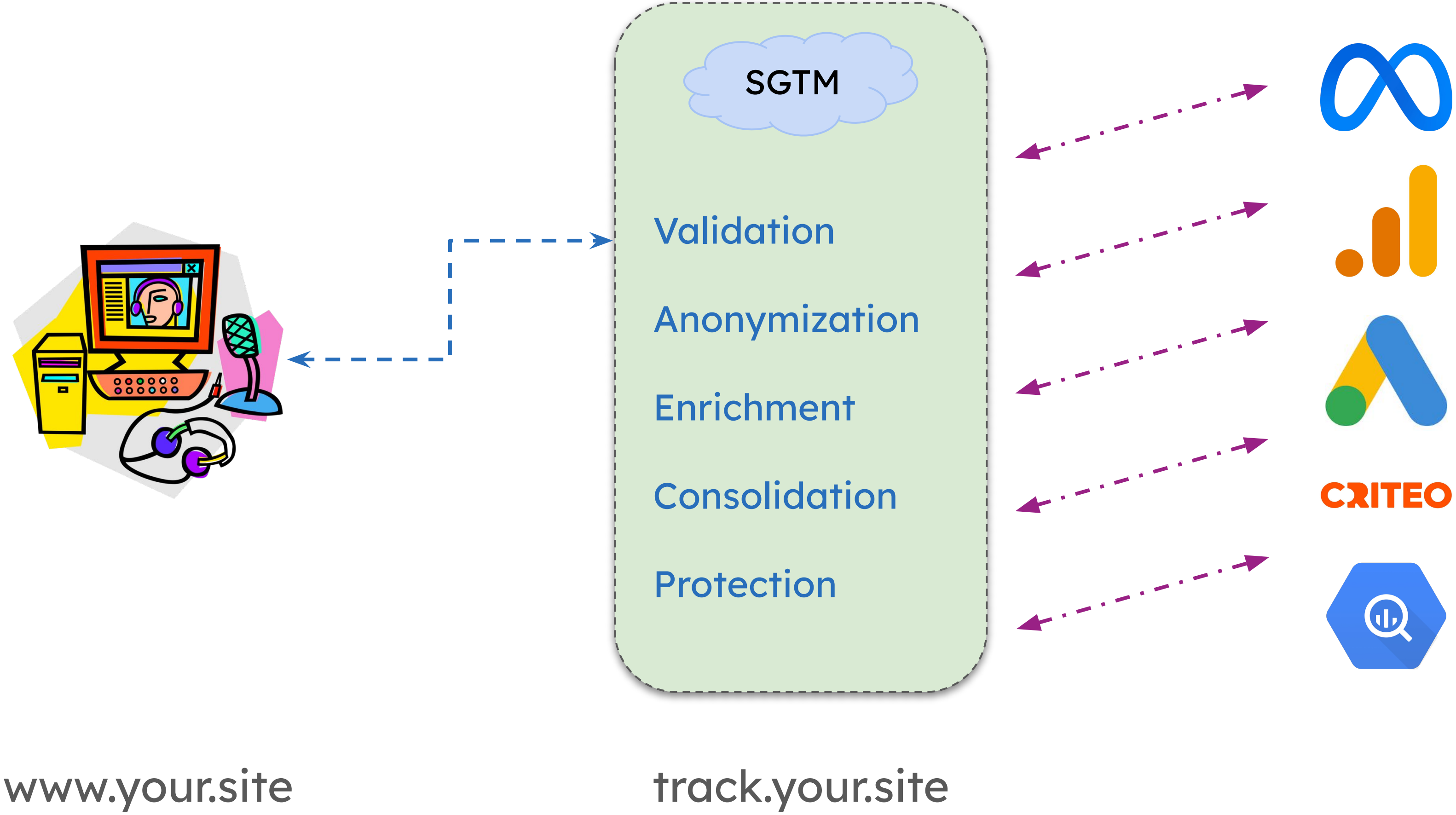
With server-side tracking, tracking is done on a separate server. The browser sends data directly to your own sGTM server and from there the data goes to the tracking tools you use.

This has the advantage that your cookies and tags are no longer blocked by the latest browsers or ad-blockers. It also provides a better user experience for your visitors because the tracking does not use your visitor's resources. Loading times are also shorter as a result.



Benefits

- ✓ **Improve page-loading time by moving your tracking tags to server-side**
- ✓ **Overall better tracking quality thanks to 1st part HTTP calls (same domain)**
- ✓ **Leverage Enhanced Conversions and Advanced Matching replacing 3rd party cookies**
- ✓ **Enable server-to-server tracking to achieve 100% tracking accuracy**
- ✓ **Get full control of dataflow to comply with business needs and privacy regulations**



SGTM

Validation

Anonymization

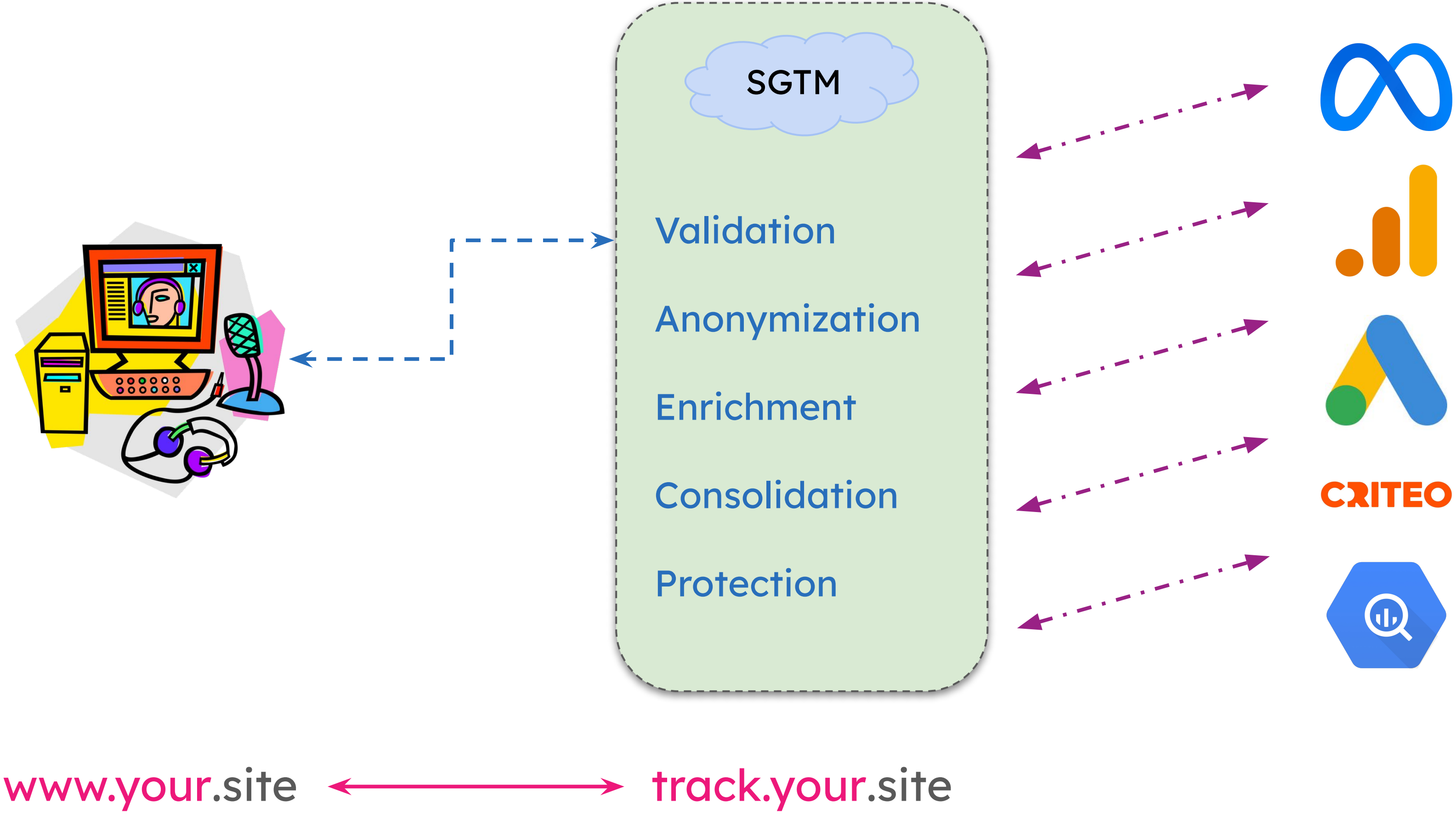
Enrichment

Consolidation

Protection

www.your.site

track.your.site



SGTM

Validation

Anonymization

Enrichment

Consolidation

Protection

www.your.site ↔ track.your.site

Wishful thinking	Reality check
Bypass ad blockers	Who doesn’t love disrespecting visitors?
Solve 3P cookies	Just…no
More, more, MORE data	It depends, and stop shouting!
1P is always better	Maybe…but is it worth it?
So… more control?	Yes! You’re getting it!

Server-side tagging is a foundation for more control. It doesn't lend itself well to data recovery, and relying on that will ultimately lead to disappointment.

The hegemony is crumbling

Analytics without GA4

Google Analytics 4 is a great tool

…if you’re using it to collect data to SGTM

…if you are happy with artificially limiting dimension cardinality

…if you’re OK with the legal and privacy risks it introduces

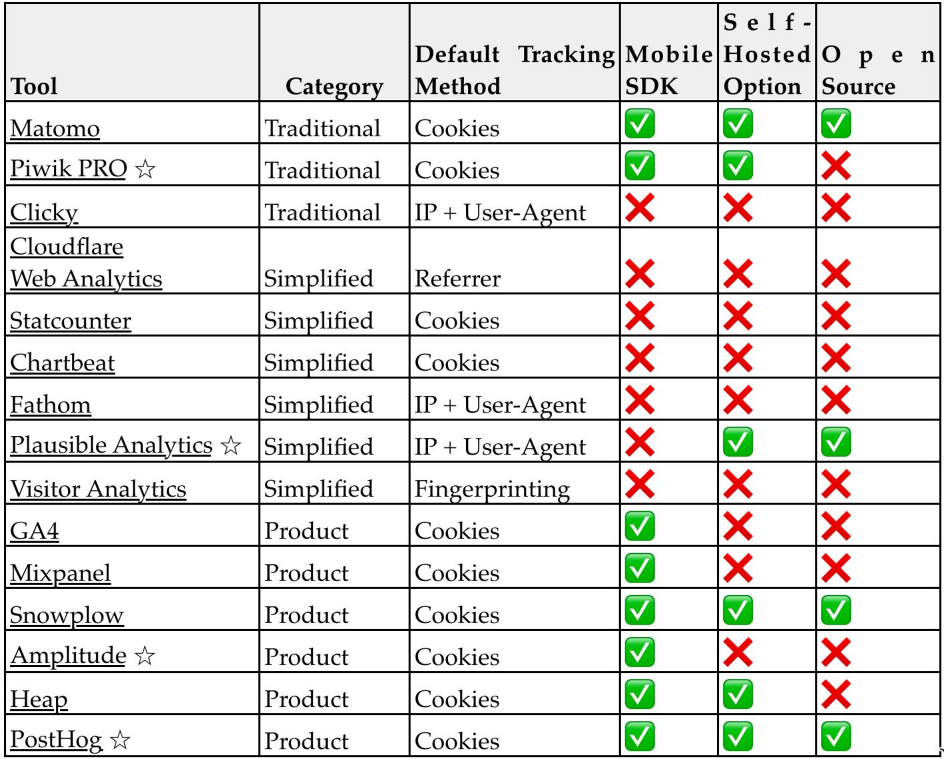
…if you’re mainly using BigQuery for analysis

…if you’re OK with unannounced and undocumented schema updates

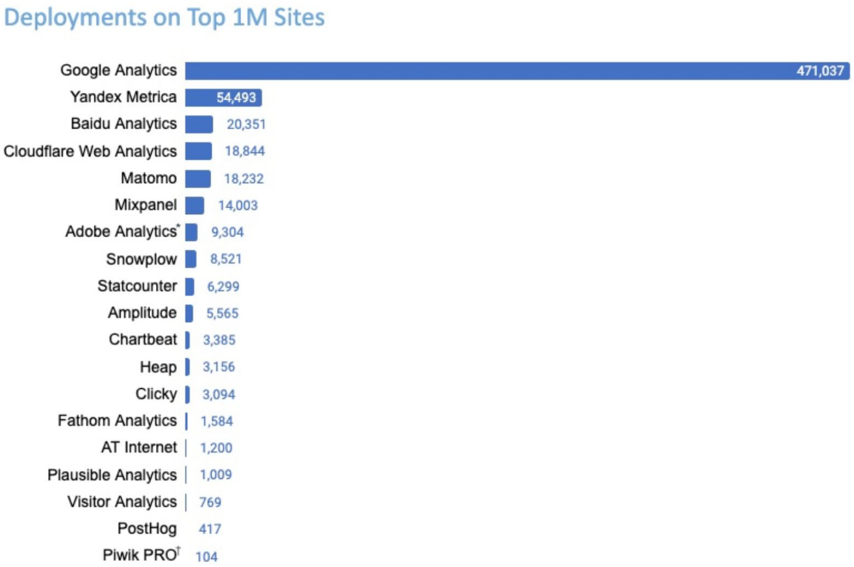
…if you get giddy with excitement when it does the bare minimum

…if you enjoy a community focused on bug hunting rather than innovation

…if you’re cool with a confusing client-side / vendor-side processing model



Tool	Category	Default Tracking Method	Mobile SDK	Self-Hosted Option	Open Source
Matomo	Traditional	Cookies	✅	✅	✅
Piwik PRO ☆	Traditional	Cookies	✅	✅	❌
Clicky	Traditional	IP + User-Agent	❌	❌	❌
Cloudflare Web Analytics	Simplified	Referrer	❌	❌	❌
Statcounter	Simplified	Cookies	❌	❌	❌
Chartbeat	Simplified	Cookies	❌	❌	❌
Fathom	Simplified	IP + User-Agent	❌	❌	❌
Plausible Analytics ☆	Simplified	IP + User-Agent	❌	✅	✅
Visitor Analytics	Simplified	Fingerprinting	❌	❌	❌
GA4	Product	Cookies	✅	❌	❌
Mixpanel	Product	Cookies	✅	❌	❌
Snowplow	Product	Cookies	✅	✅	✅
Amplitude ☆	Product	Cookies	✅	❌	❌
Heap	Product	Cookies	✅	✅	❌
PostHog ☆	Product	Cookies	✅	✅	✅



Google Analytics Alternatives *(Jason Packer)*

Google Analytics 4 is a good tool. Honestly. But you are in no way obligated to use it or to stick with it. Do yourself and your organization a favor and shop around.

You should have stopped with the pain

2 x Founder / Partner	Simmer, 8-bit-sheep
Blogger	simoahava.com, teamsimmer.com
Community no-lifer	https://join.measure.chat/
Twitter	https://www.twitter.com/SimoAhava
Mastodon	https://masto.measure.chat/@SimoAhava

```
log(`Thank you, ${yourName}`)
```