Server-side Tracking

Myth of the “cookieless” future
Simo Ahava
Partner, co-founder: @Team_Simmer and @8_Bit_Sheep
Blogger, developer: www.simoahava.com
Twitter: @SimoAhava
Curator: www.cookiestatus.com
Definitions:
“Regular” tagging
“Regular” tagging

from @Team_Simmer for FoS22
“Regular” tagging
“Regular” tagging

HTTP Request

HTTP Response

from @Team_Simmer for #FoS22

Server-side Tracking
“Regular” tagging

HTTP Request
- Reliant on 3P CDN
- Privileged access
- Cross-site tracking
- Data transfer laws
- PII leaks / XSS vectors

HTTP Response

from @Team_Simmer for #FoS22
Definitions:
Server-side tagging
Server-side tagging

from @Team_Simmer
for #FoS22
Server-side tagging

Server container

from @Team_Simmer for #FoS22
Server-side tagging

Server container
Hit validation
Stream consolidation
Anonymization
Data flow control
Client-side perf
Tracking protection

from @Team_Simmer for #FoS22
What happens in the server, stays in the server.
Server-side gives organizations **full control** over the upstream data flows and allows them to **selectively validate** and **enrich** the data that is shipped to vendors.
Controls for *full anonymization* of the data stream
Portable solution, runs on **Docker**
Server-side lets organizations **hide and manipulate** the data streams in ways that might violate the **trust** of the user and the **legal bases** for processing their (personal) data.
### Opaque data collection

<table>
<thead>
<tr>
<th>Status</th>
<th>Method</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>POST</td>
<td><a href="http://www.google-analytics.com">www.google-analytics.com</a></td>
</tr>
<tr>
<td></td>
<td>GET</td>
<td><a href="http://www.google-analytics.com">www.google-analytics.com</a></td>
</tr>
<tr>
<td></td>
<td>GET</td>
<td><a href="http://www.google-analytics.com">www.google-analytics.com</a></td>
</tr>
<tr>
<td>200</td>
<td>GET</td>
<td>sgtn.simoahava.com</td>
</tr>
<tr>
<td>200</td>
<td>GET</td>
<td>sgtn.simoahava.com</td>
</tr>
</tbody>
</table>
Server-side can have amazing **client-side performance** benefits, as heavy, expensive third-party JavaScript libraries and pixel requests can be offloaded to the server.
Server-side lacks proper controls for allowing **validation** and **auditing** of data flows from the **client**. Only those with access to the server can **report** what is being done.
Server-side lets you move to a **first-party only** setup, where user data cannot be **harvested** by vendors using **third-party cookies** or **unchecked** scripts.

from @Team_Simmer for #FoS22
Server-side might tempt companies to send ("hashed") identifying bits to vendors due to lack of proper matching signals using just (pseudonymous) identifiers.
Server-side is a paradigm for **companies** to gain more **control** over what data **vendors can process** from the companies’ customers.
Server-side is a paradigm for **companies** to gain more **control** over what data **vendors can process** from the companies’ customers.

By moving the data flows **away** from the **client**, users/customers lose **agency** and control over their data.
Summa summarum...
Server-side...
Server-side...

- **Can be** an amazing asset to help secure data flows in a privacy-first world
Server-side...

- **Can be** an amazing asset to help secure data flows in a privacy-first world
- **Is** a great way to reduce client-side bloat and introduce data enrichment at scale
Server-side...

- Can be an amazing asset to help secure data flows in a privacy-first world
- Is a great way to reduce client-side bloat and introduce data enrichment at scale
- Should not be considered a way to circumvent consent and ad blockers, or to erode user agency
Server-side...

- **Can be** an amazing asset to help secure data flows in a privacy-first world
- **Is** a great way to reduce client-side bloat and introduce data enrichment at scale
- **Should not** be considered a way to circumvent consent and ad blockers, or to erode user agency
- **Is not** a silver bullet that helps solve all data-related issues in 2022; it’s a *surgical tool*, not a *panacea*
Server-side...

- **Can be** an amazing asset to help secure data flows in a privacy-first world
- **Is** a great way to reduce client-side bloat and introduce data enrichment at scale
- **Should not** be considered a way to circumvent consent and ad blockers, or to erode user agency
- **Is not** a silver bullet that helps solve all data-related issues in 2022; it’s a *surgical tool*, not a *panacea*
- **Should be** something that all companies working with client-side data investigate and research for compatibility with their own data practices

from @Team_Simmer for #FoS22
Further reading
Resources...

My articles:
https://www.simoahava.com/tags/server-side-tagging/

Official documentation:
https://developers.google.com/tag-platform/tag-manager/server-side

Overview video:
https://www.youtube.com/watch?v=6OGbOh216mU

Course on the Simmer platform:
https://www.teamsimmer.com/courses/server-side-tagging/
log(Thank you ${yourName}`)