Privacy + Security Forum

Session:
Tracking Technology Deep Dive

Privacy+ Security Forum

Speakers: Tracking Technology Deep Dive

R. Jason Cronk
Attorney,
Microdesic Law, PLLC

Andrew Berry
Privacy Engineer
Enterprivacy
Consulting Group

Privacy+ Security Forum

Discussion

Why are there issues with web tracking that are not just about cookies?

Privacy+ Security Forum

EXERCISE

Wiretap claims can be brought under a number of laws:

1. Federal Wiretap Act/Electronic Communications in Privacy Act (ECPA)
2+. California Invasion of Privacy Act (CIPA)
2+. Florida Security in Communications Act (FSCA)
?. Other state laws

For an interception claim, broadly, there must be:

- a communication
- capture of that communication

EXERCISE

Scenario 1:
A 3rd party JavaS ebtag is triggered whe **nts** a registratio ation from the Em ured by the scrip

Probably interception

Scenario 2:
A 3rd party J d webtag is triggere **enters** their email . Information fro eld is captured by the

Probably not interception

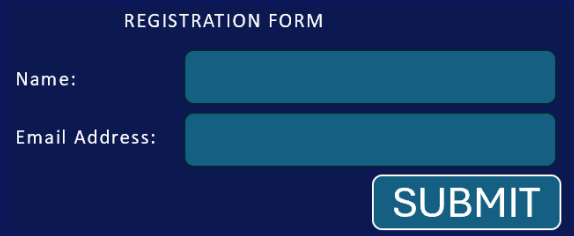
REGISTRATION FORM

Name: Jason

Email Address: Jason@example.com

SUBMIT

EXERCISE



Captured when "Submit" button clicked

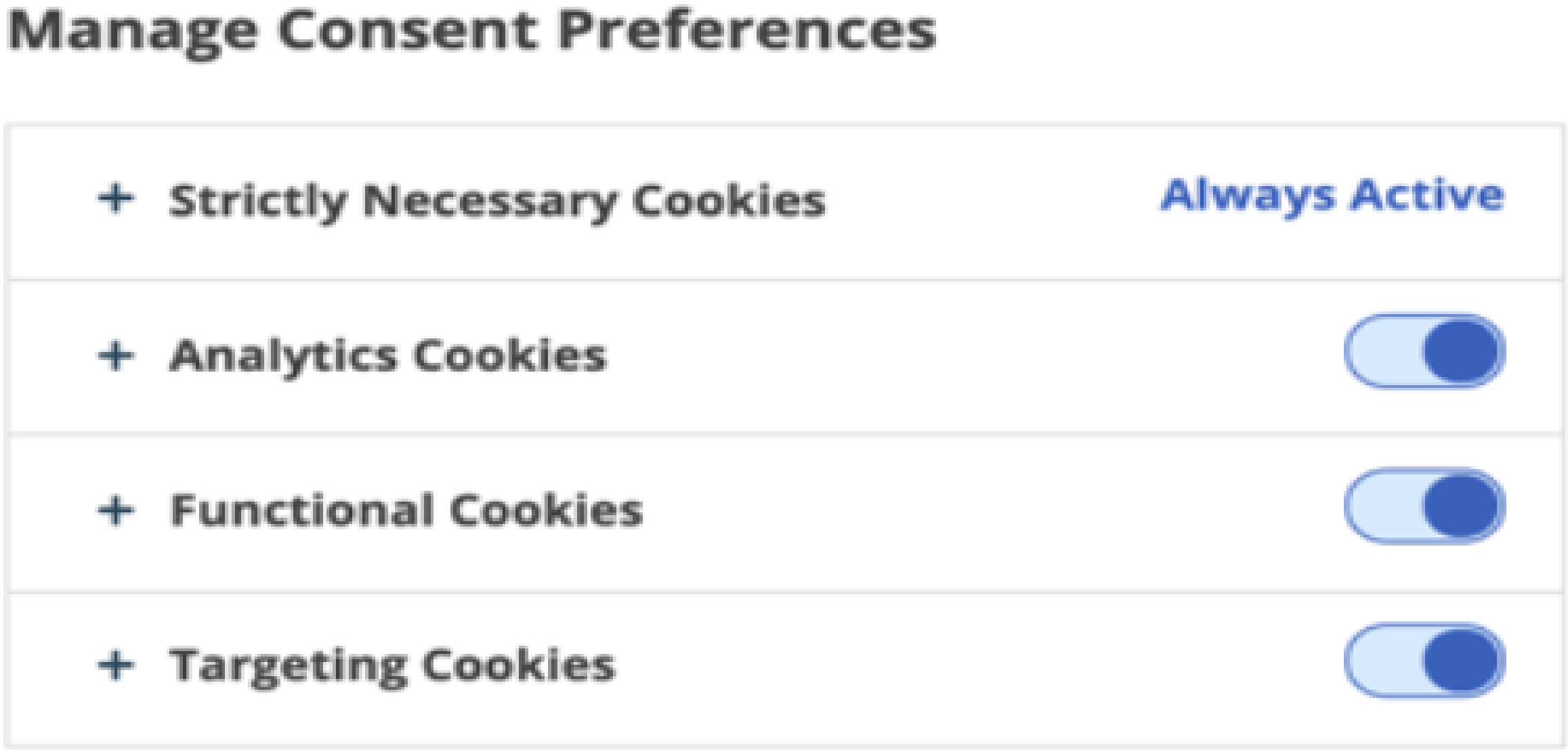
Captured when entered in the form

Probably interception

Probably Not interception

What if the 3rd party script captures when entered *but the website is also capturing that information before the Submit button is pressed*?

EXERCISE


Manage Consent Preferences
+ Strictly Necessary Cookies
Always Active
+ Analytics Cookies
+ Functional Cookies
+ Targeting Cookies

Cookies

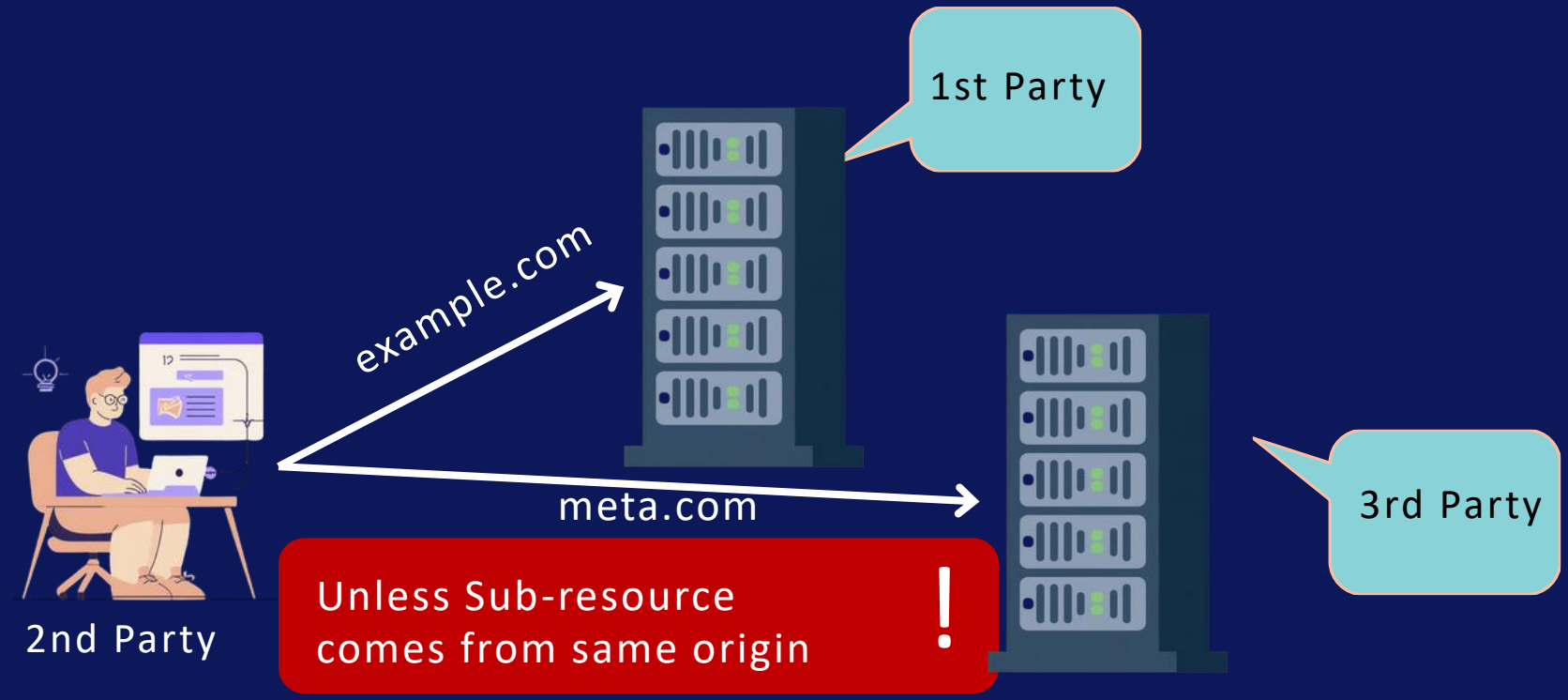
Cookies refer to chunks of data stored by a web browser as name value pairs. They can be stored in files or in a database.

Privacy+ Security Forum

COOKIES

Cookies can be **written** or **read** by:

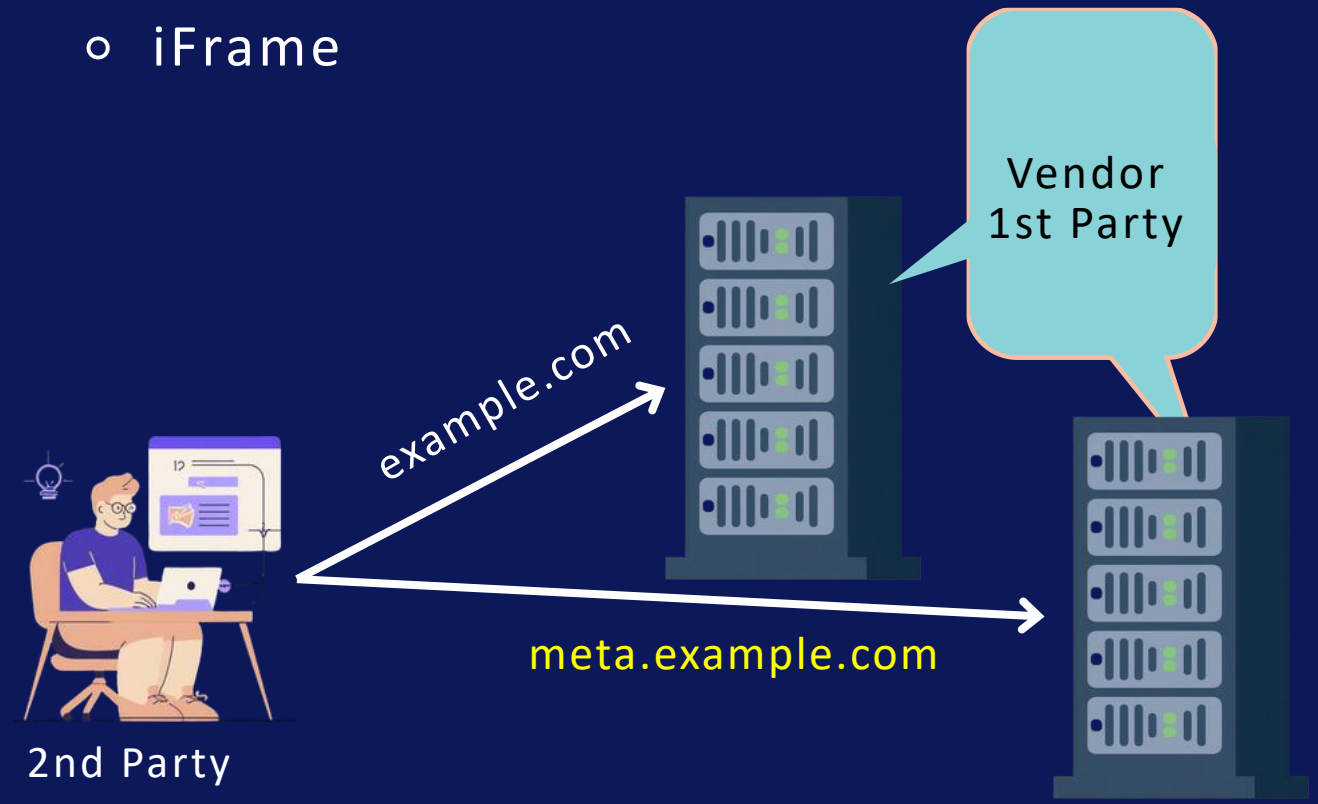
- Main resource (i.e. the webpage)
- Sub-resource
  - Image
  - JavaScript
  - iFrame



COOKIES

Cookies can be **written** or **read** by:

- Main resource (i.e. the webpage)
- Sub-resource
  - Image
  - JavaScript
  - iFrame



COOKIES

Cookies can be **written** by:

- HTTP Response Header:
  - *Set-Cookie: username=jason*
- JavaScript:
  - *document.cookie=”username=jason”;*

Cookies can be **read** through:

- HTTP Request Header:
  - *Cookie: username=Jason*
- JavaScript:
  - *Let x = document.cookie;*

COOKIES

- **Persistence** - cookies can expire, using *Max-Age* or *Expires* attributes
  - Upon window closure
  - At some time in the future
  - Never
  - Immediately (to delete cookie)

- **Security Features**
  - Domain – cannot be accessed by other domains
  - Secure – cannot be access over unsecure HTTP
  - Httponly - cannot be accessed by JavaScript
  - and others...

Not Cookies

Not all Webtags drop cookies.

Privacy+ Security Forum

TRACKING TECHNOLOGY

Tracking technology is a broad term for any technology that collects data about the user.

TAG

A piece of code on a webpage

<image src=”example.com/image.png”/>

<script src=”example.com/phonehome.js”/>

<iframe src=”example.com/innerPage.html”/>

DIFFERENT TYPES OF “TAGS”

*An **HTML Tag** refers to the markup of elements in a webpage (i.e. the <></>)*

*A **Meta Tag** refers to information in the header of an HTML document*

```
<head>
  <meta name="description" content="My Website"\>
  <meta name="keywords" content="web, beacons, tags"\>
</head>
```

*A **Web Tag** refers to code used for analytics, tracking or advertising purposes.*

BEACON

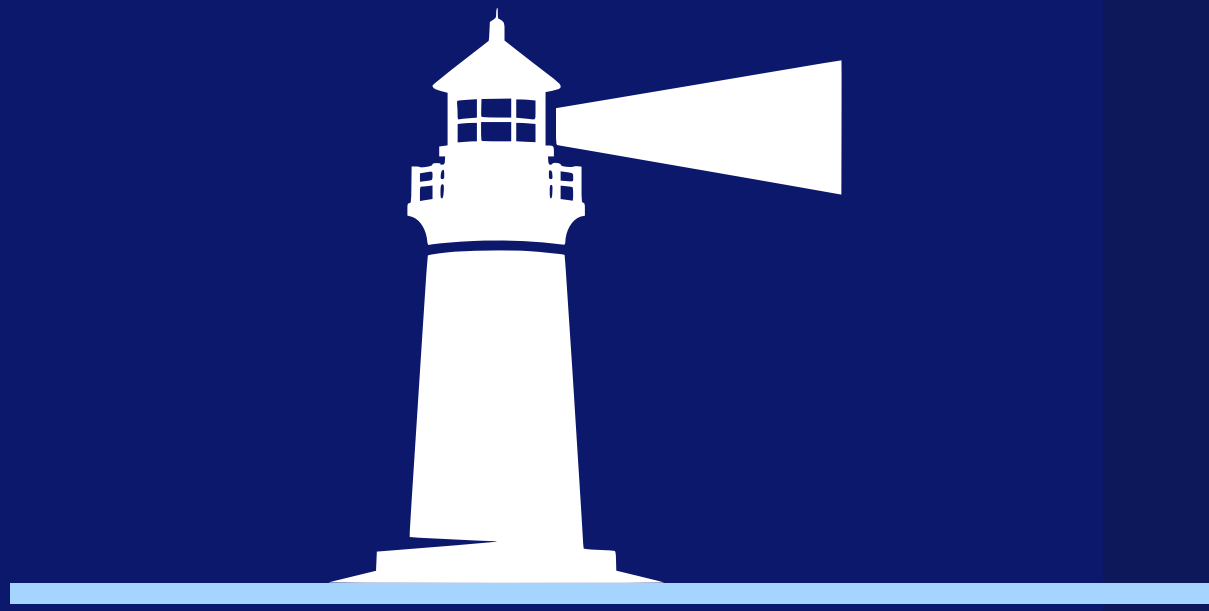
Beacon and webtag are often used interchangeably but technically a webtag need not send information to a company

A **beacon** *is a generic term for a snippet of HTML code, that sends a signal/information to a company. It can be*

- *an image*
- *JavaScript*
- *an iFrame*

Pixel

an image based webtag

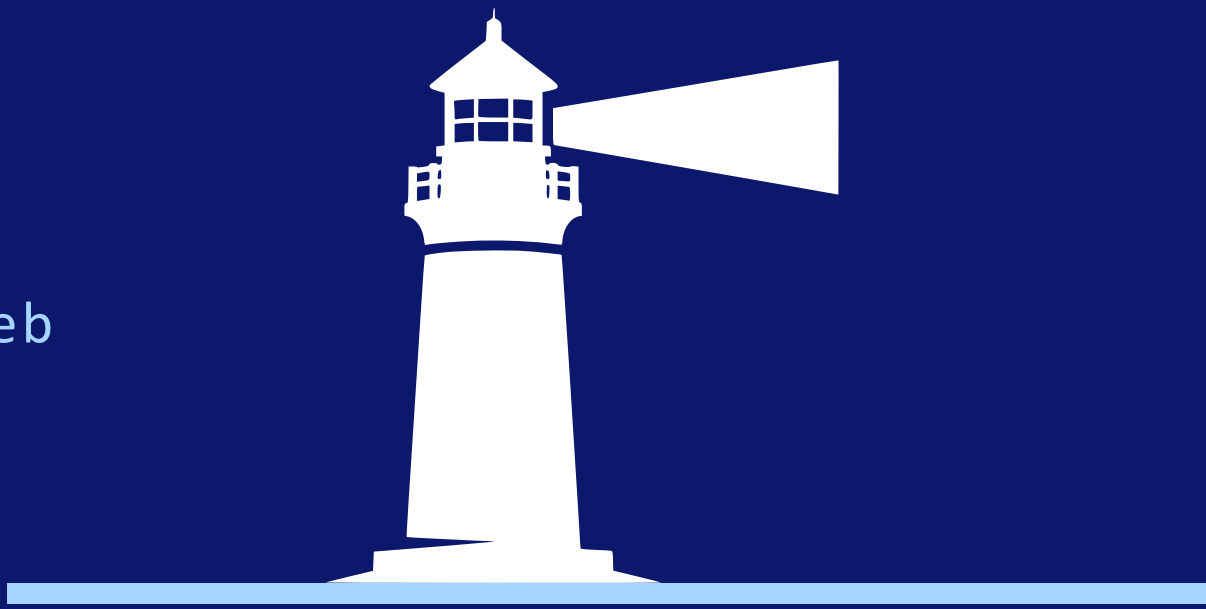


<image src=”example.com/image.png?user=Jason” width=1 height=1/>

Sources of data:
IP address
URL query string
Request Header

JAVASCRIPT

Code to be executed by a Web Browser



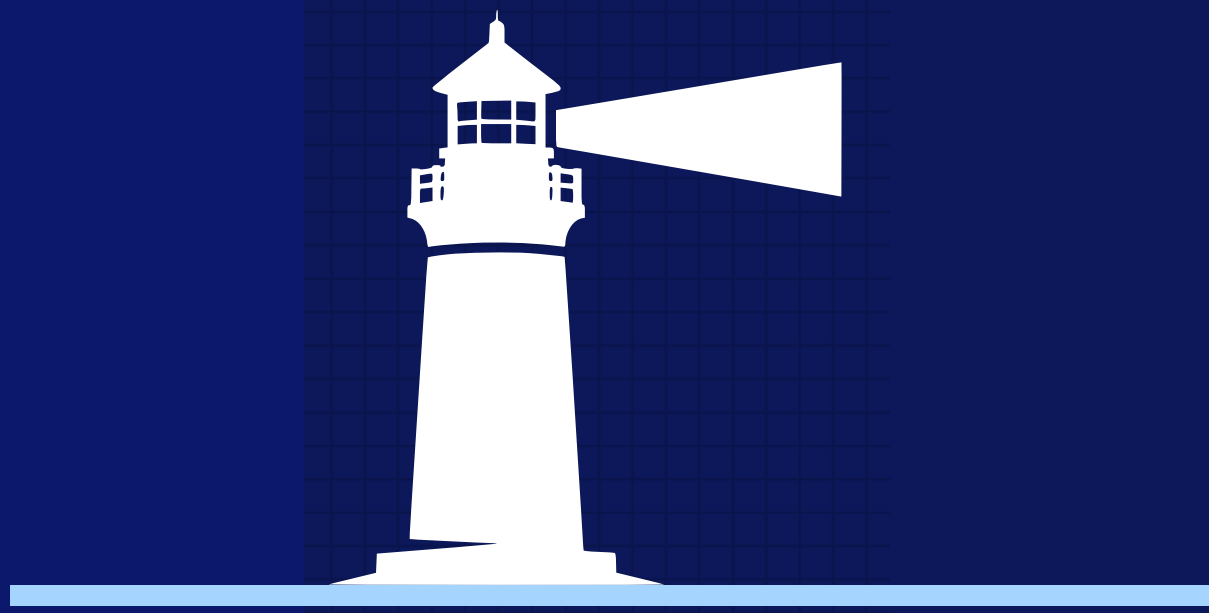
```
<script src=”example.com/phonehome.js”/>
<script>
        var height = window.screen.height;
        var width = window.screen.width;?var isChrome = !!window.chrome;
</script>
```

Sources of data (obtained by Code):

- Browser context (window size, type of browser, plugins, etc.)
- State of the webpage
- Monitor events (mouse clicks, keystrokes, etc.)

IFRAME

A way to include another webpage in a webpage



<iframe src=”example.com/innerPage.html”/>

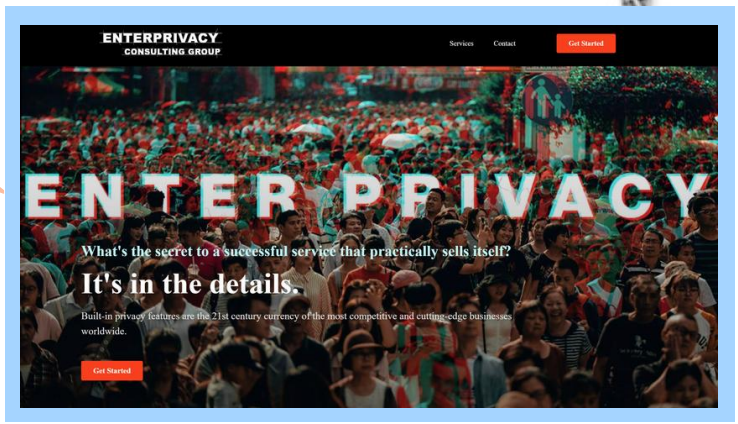
Active tab

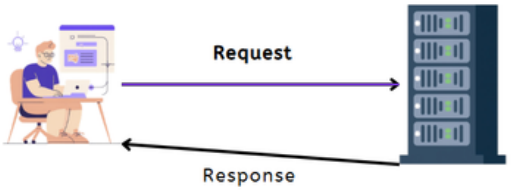
Background tab

Hello World. This is my webpage!

parent

iframe





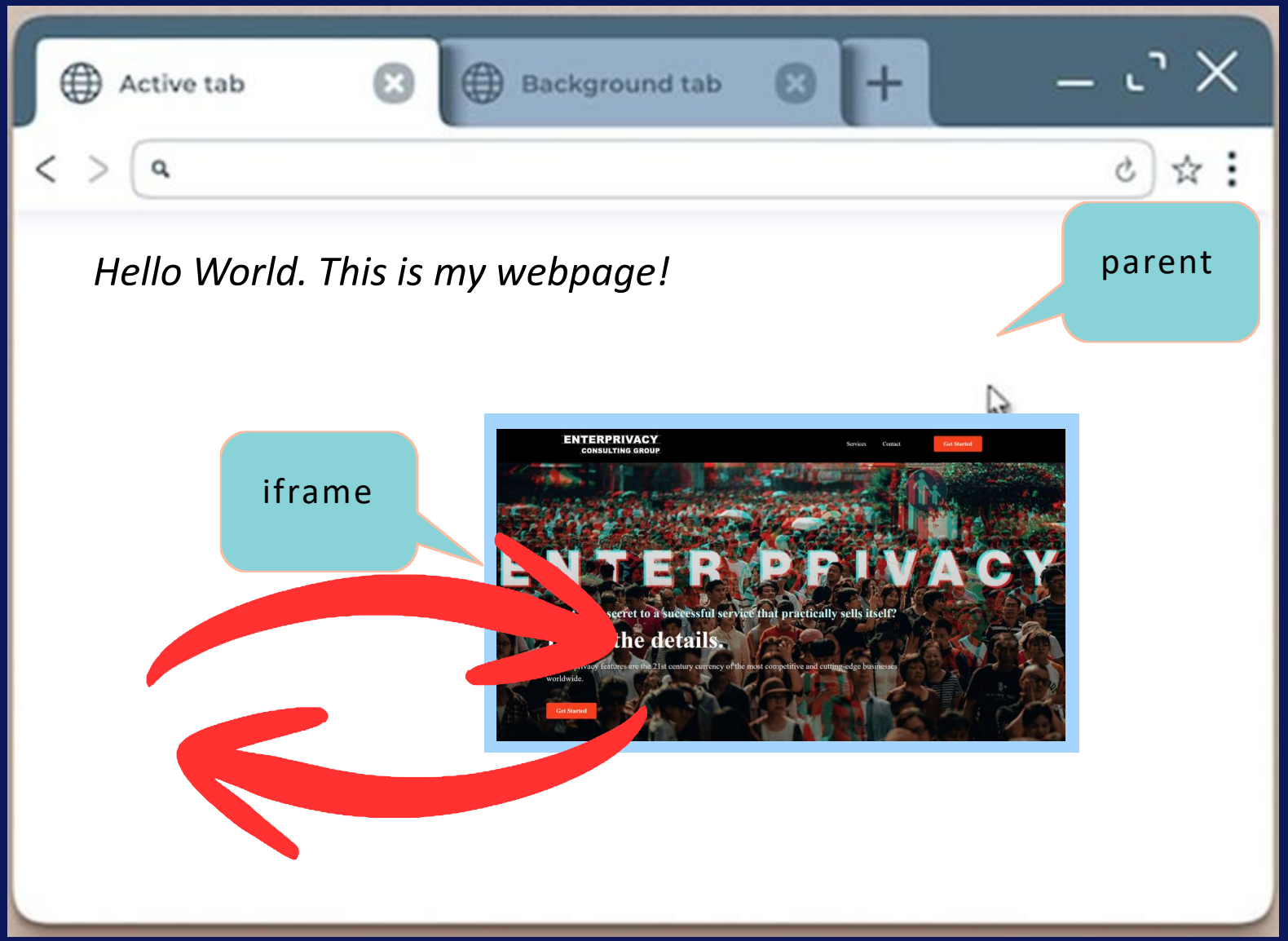
IFRAME

<iframe src="example.com/innerPage.html?user=Jason"/>

Sources of data:
IP address
URL query string
Request Header
Request Payload

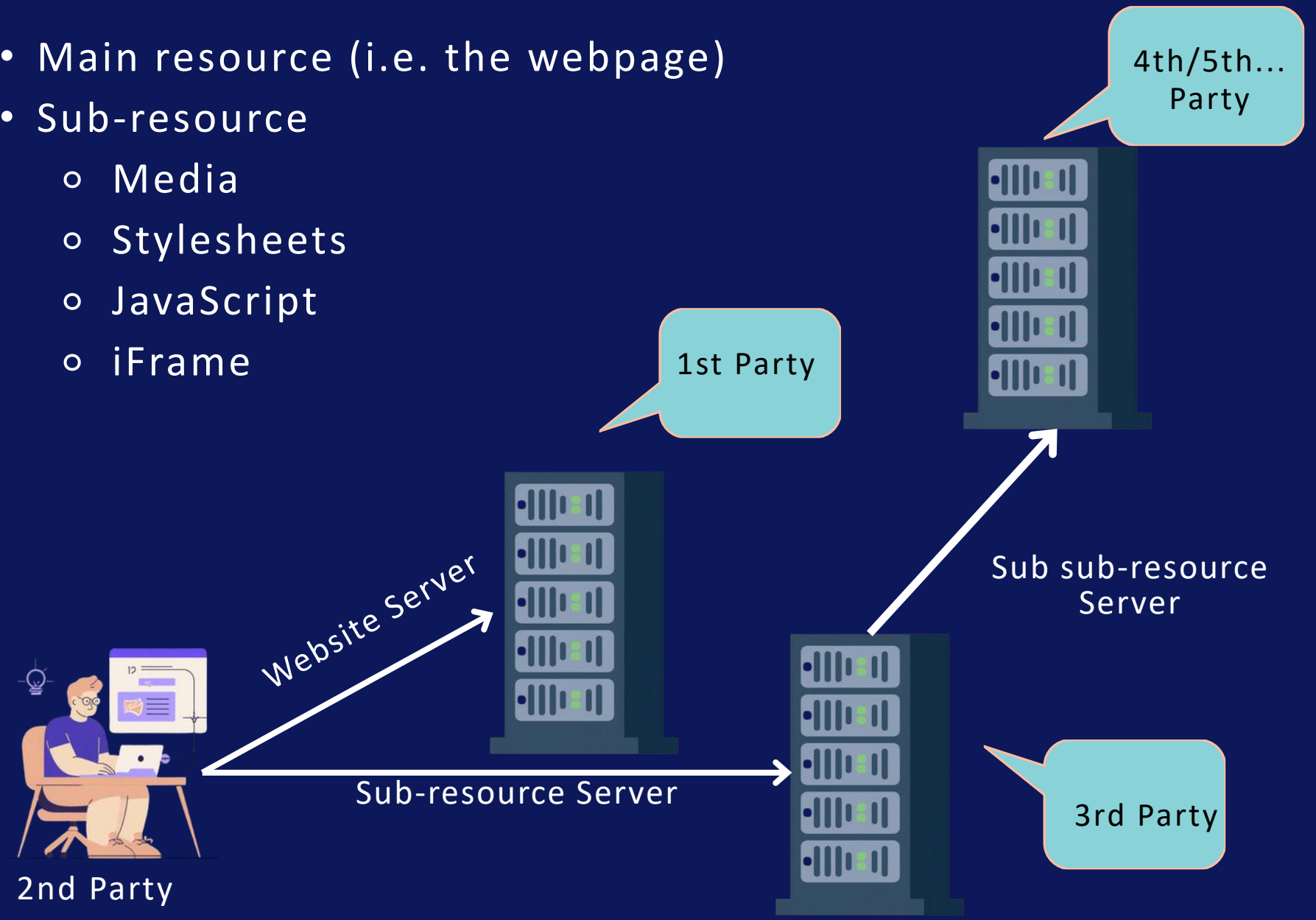
from JavaScript:

- Browser context (window size, type of browser, plugins, etc.)
- State of the webpage
- Monitor events (mouse clicks, keystrokes, etc.)


Active tab
Background tab
Hello World. This is my webpage!
parent
iframe
ENTERPRIVACY
CONSULTING GROUP
Services
Contact
Get Started
ENTERPRIVACY
secret to a successful service that practically sells itself?
the details.
worldwide.
Get Started

PARTIES

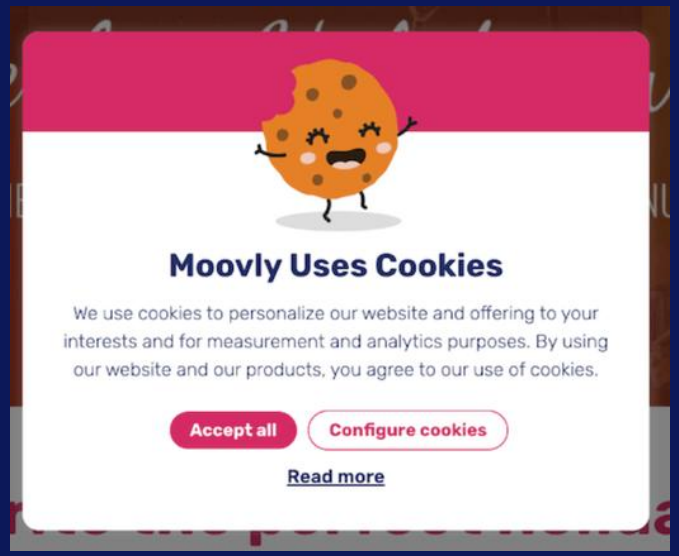
- Main resource (i.e. the webpage)
- Sub-resource
  - Media
  - Stylesheets
  - JavaScript
  - iFrame



TAG MANAGER

A **Tag Manager** is software run on a webserver to help orchestrate which tags are shown on which websites under which conditions.

CONSENT MANAGEMENT PLATFORMS



- Came into prominence late 2010's after GDPR came into effect.
- Mostly a result of EU's E-Privacy Directive which requires consent for storing of files on a user's computer.
- Cookies ≠Webtags/Beacons (which may or may not write cookies)
- CMPs don't actually block cookies, they block the code that writes cookies (i.e. Webtags/Beacons).
- CMPs usually save users preferences by ..... usually writing cookies to the user's machine.

CONSENT MANAGEMENT PLATFORMS

CMPs don’t actually block cookies, they block the code that writes/reads cookies.

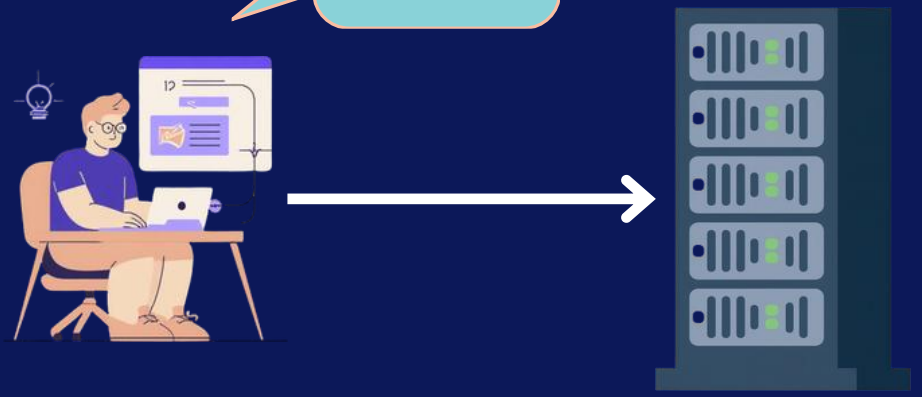
Set before CMP

Can be blocked by CMP

Cookies can be written or read by:

- Main resource (i.e. the webpage)
  - HTTP Response Header: 🚫
    - Set-Cookie: username=jason
  - JavaScript: ✅
    - document.cookie=”username=jason”;
- Sub-resources
  - Image
  - JavaScript
  - iFrame

CMP runs in browser*



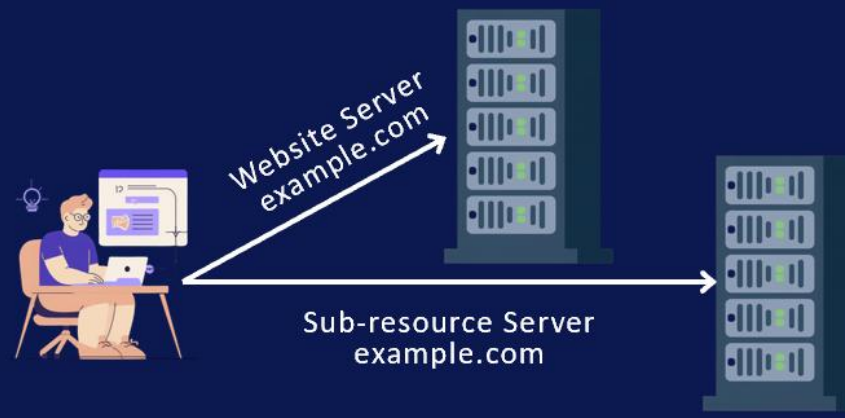
CONSENT MANAGEMENT PLATFORMS

CMPs don’t actually block cookies, they block the code that writes/reads cookies.

Cookies can be written or read by:

- Main resource (i.e. the webpage)
  - HTTP Response Header 🚫
  - JavaScript ✅

- Sub-resources
  - Image
    - HTTP Response Header ✅ (Do not load)
  - JavaScript ✅
  - iFrame
    - HTTP Response Header ✅ (Do not load iFrame)
      - Advanced: run through a proxy
    - JavaScript ✅ (Do not load iFrame)
      - Advanced: run through a proxy
      - Advanced: pass consent preferences

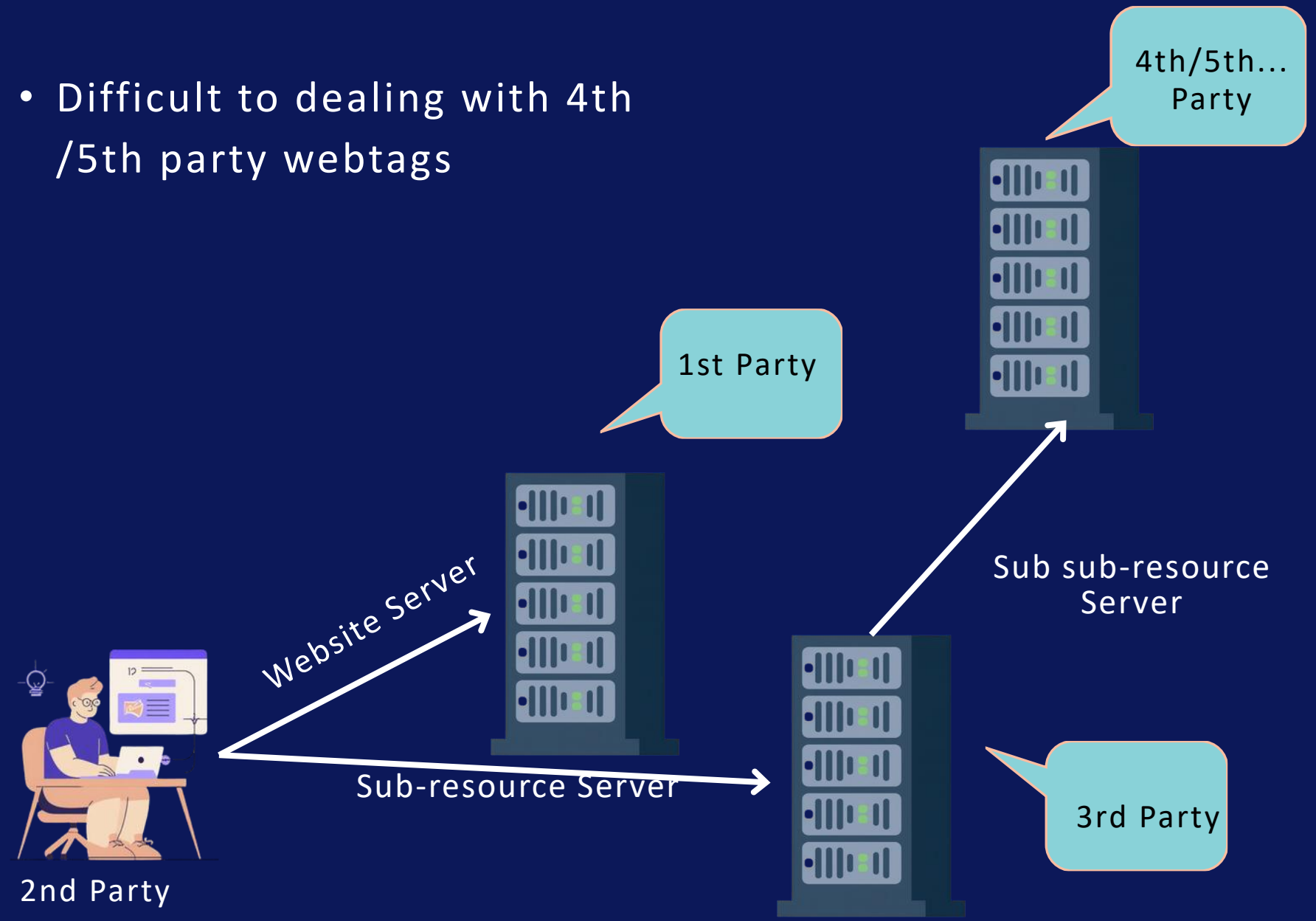


Known Issues with CMPs

- Once cookies are placed, the CMP cannot (generally) remove cookies
  - It can disable scripts, preventing further read/writes from that website
  - This does not prevent the cookie from being read by a script on another website (assuming same-origin policy)

Known Issues with CMPs

- Difficult to dealing with 4th /5th party webtags



Known Issues with CMPs

- Focusing on cookies
- Timing: Cookie/Webtag triggered before CMP
- Configuration/management issues
  - Mislabeling (i.e. functional/performance/"necessary")
    - Also, multi-purpose Webtags
  - Failed integration
    - Integrated with Tag Manager but then rogue WebTag on random webpage on site that isn't managed by Tag Manager
    - No Tag Manager
  - Evolving website requires constant maintenance

GLOBAL PRIVACY CONTROL

The Global Privacy Control (GPC) is a signal sent from a web browser during an HTTP Request that tells the server the user does not want their data share or sold*

```
GET / HTTP/1
Host: example.com
Sec-GPC: 1
```

Currently only supported in some browsers by default (Brave) and with some plugins

*Actual meaning may vary.

GLOBAL PRIVACY CONTROL INTERPRETATION ISSUES

GPC is meant to be a manifestation of an express declaration of the user to not sell/share their data. Ubiquity (by default) might vacate user intent.

Important!

Currently only supported in some browsers by default (Brave) and with some plugins

California Opt Me Out Act (AB 566)

Requires all browsers to support (though not have default opt-out)

GLOBAL PRIVACY CONTROL INTERPRETATION ISSUES

- GPC signal does not have legal implication in every jurisdiction
- GPC signal does not mean you cannot set cookies
- GPC signal does not mean you cannot use WebTags/Beacons
- GPC signal does not mean you cannot use data for specific purposes
- THIS does not map well to consent banners which often model consent based on cookies and purposes

GPC signal DOES means the user opts out of the selling or sharing of their data (in certain jurisdictions)

Complexities
- Integration with CMPs (technically easy), are complex from a management perspective
- Cross device/cross account interpretation
- Integration with “Do not sell my data” forms
- Backend selling/sharing

Stay in touch: Continue the conversation with us

R. Jason Cronk, Esq.
Microdesic Law, PLLC
rjcesq@microdesic.com

Andrew Berry
Enterprivacy Consulting Group
anberry@enterprivacy.com

Privacy+ Security Forum