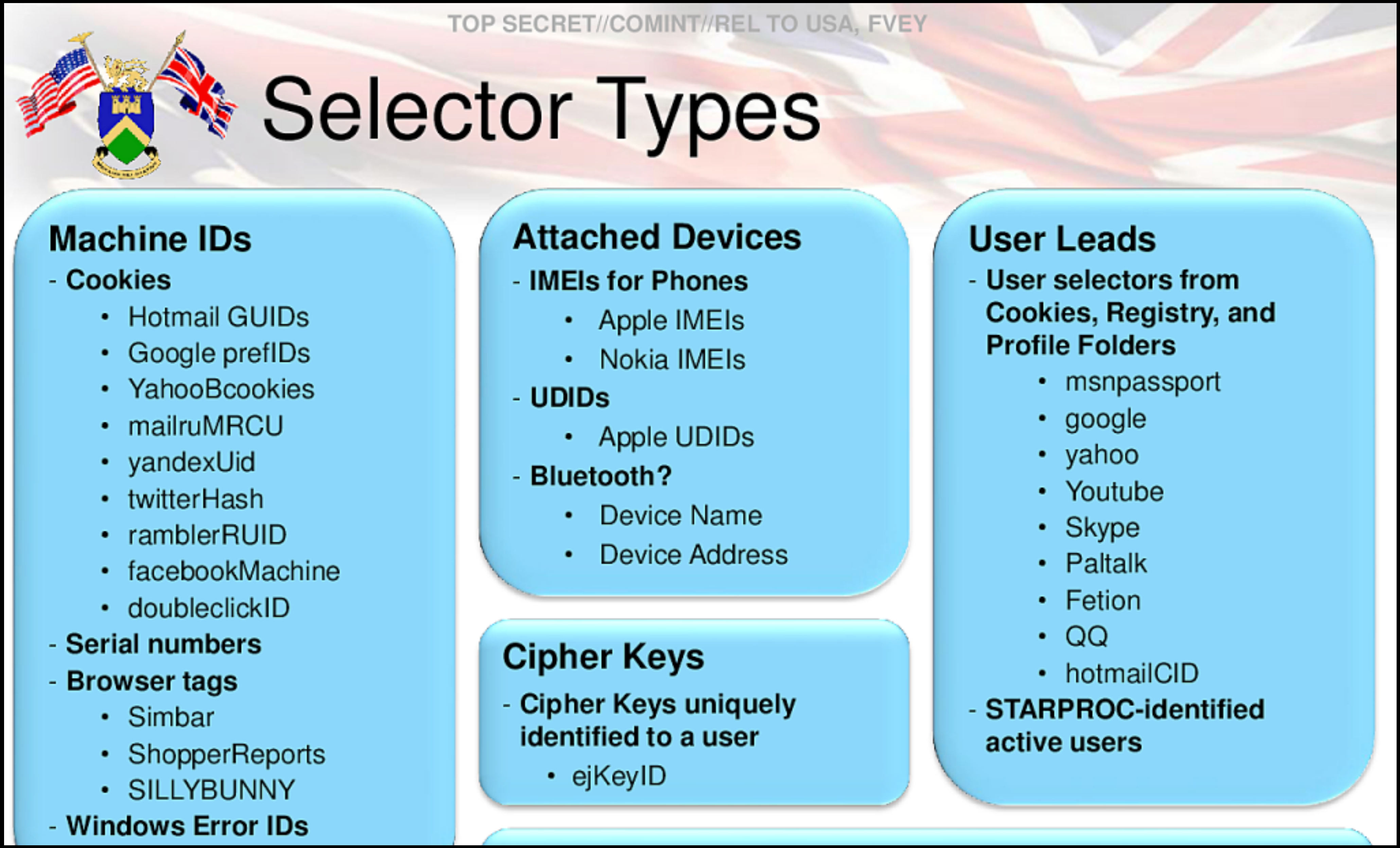
Can We
Protect Privacy
Without Breaking the Web?



TOP SECRET//COMINT//REL TO USA, FVEY

Selector Types

Machine IDs

- Cookies
  - Hotmail GUIDs
  - Google prefIDs
  - YahooBcookies
  - mailruMRCU
  - yandexUid
  - twitterHash
  - ramblerRUID
  - facebookMachine
  - doubleclickID
- Serial numbers
- Browser tags
  - Simbar
  - ShopperReports
  - SILLYBUNNY
- Windows Error IDs

Attached Devices

- IMEIs for Phones
  - Apple IMEIs
  - Nokia IMEIs
- UDIDs
  - Apple UDIDs
- Bluetooth?
  - Device Name
  - Device Address

Cipher Keys

- Cipher Keys uniquely identified to a user
  - ejKeyID

User Leads

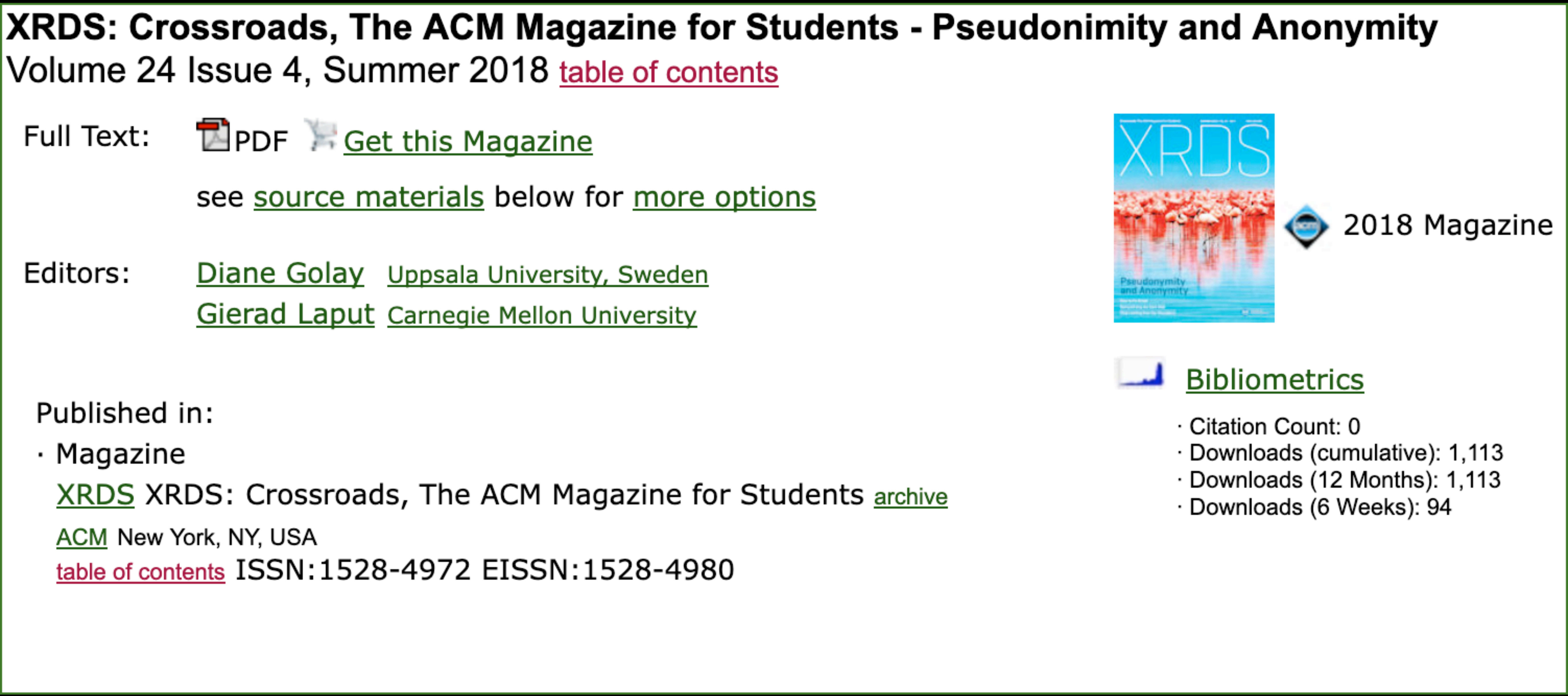
- User selectors from Cookies, Registry, and Profile Folders
  - msnpassport
  - google
  - yahoo
  - Youtube
  - Skype
  - Paltalk
  - Fetion
  - QQ
  - hotmailCID
- STARPROC-identified active users

Leaked documents show that the NSA uses tracking cookies to select targets

Image: The Intercept
https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/

I DON'T EVEN KNOW
HOW I GOAT HERE

Background on current web architecture



XRDS: Crossroads, The ACM Magazine for Students - Pseudonimity and Anonymity
Volume 24 Issue 4, Summer 2018 table of contents

Full Text: PDF Get this Magazine

see source materials below for more options

Editors: Diane Golay Uppsala University, Sweden
Gierad Laput Carnegie Mellon University

2018 Magazine

Bibliometrics

- Citation Count: 0
- Downloads (cumulative): 1,113
- Downloads (12 Months): 1,113
- Downloads (6 Weeks): 94

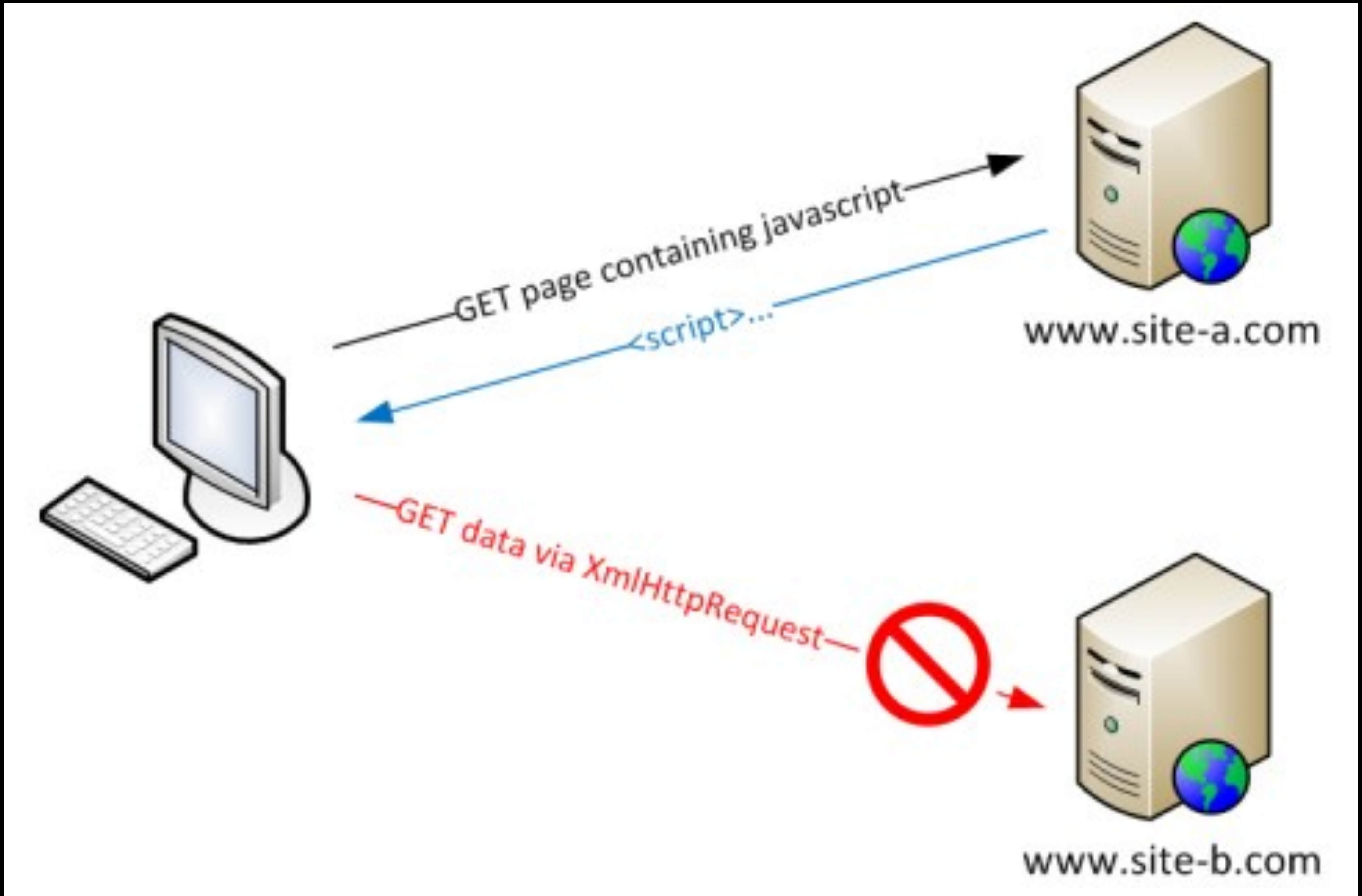
Published in:

- Magazine

XRDS XRDS: Crossroads, The ACM Magazine for Students archive
ACM New York, NY, USA
table of contents ISSN:1528-4972 EISSN:1528-4980

"As a first line of defense to preserve user privacy, all major web browsers adhere to the guidelines of the ***same origin policy***, which limits a website's access to information."

Same-origin Policy



http://www.lucadentella.it/en/2013/07/11/javascript-same-origin-policy-e-jsonp/

Cross-Origin Request code

```
http://www.evilcorp.com

<html>
 …
   <script>
    new XMLHttpRequest().open(
      “GET”, “boss.bankofamerica.com/data.json”
    );
   </script>
 …
</html>
```

https://speakerdeck.com/groovecoder/top-5-security-errors-we-see-from-firefox-and-how-to-fix-them

Cross-Origin Request Threats

Attacker

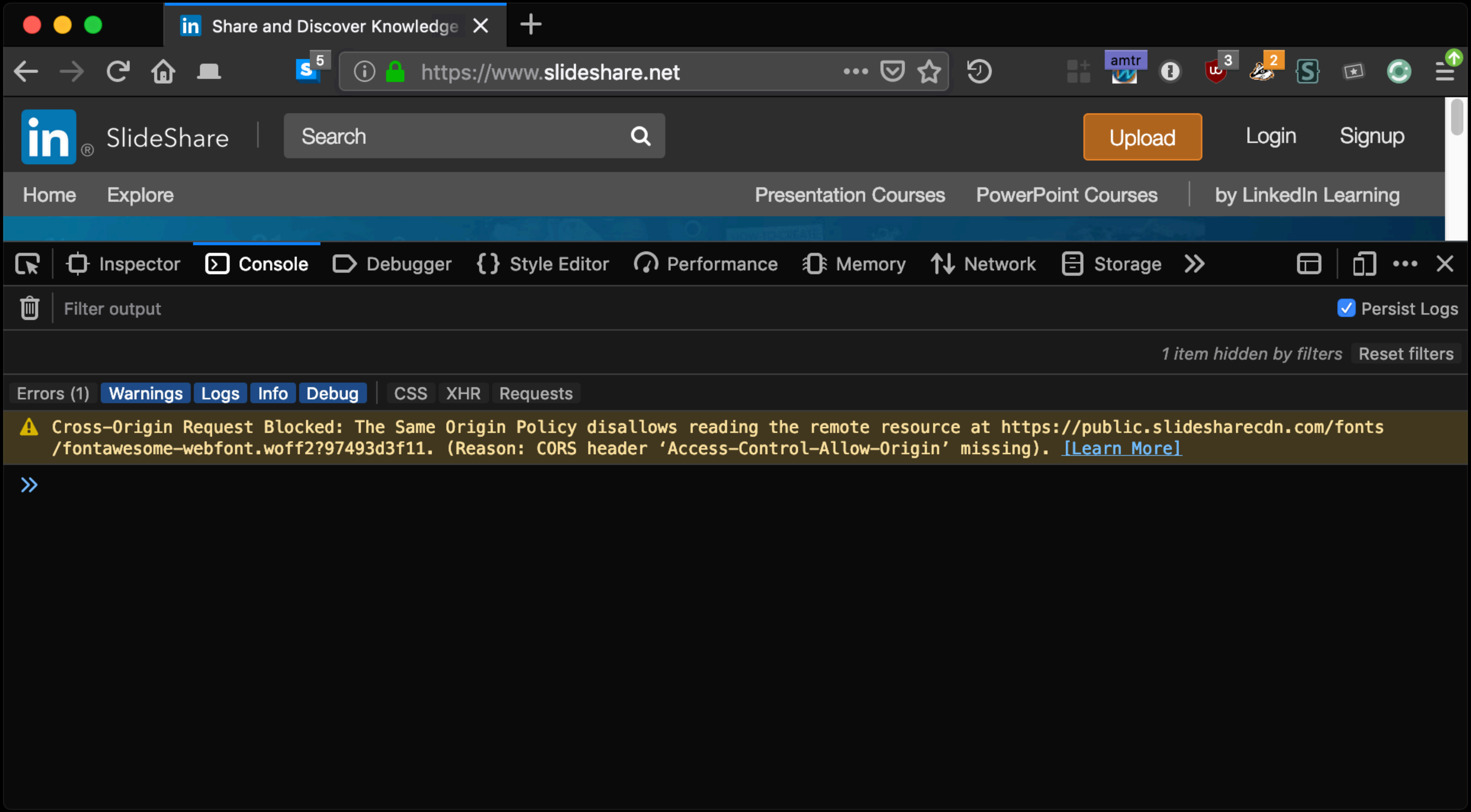
- *Any* Malicious Origin
  - Phishing & Malware Sites
  - Compromised CDNs
  - Untrusted First Parties

Attacks

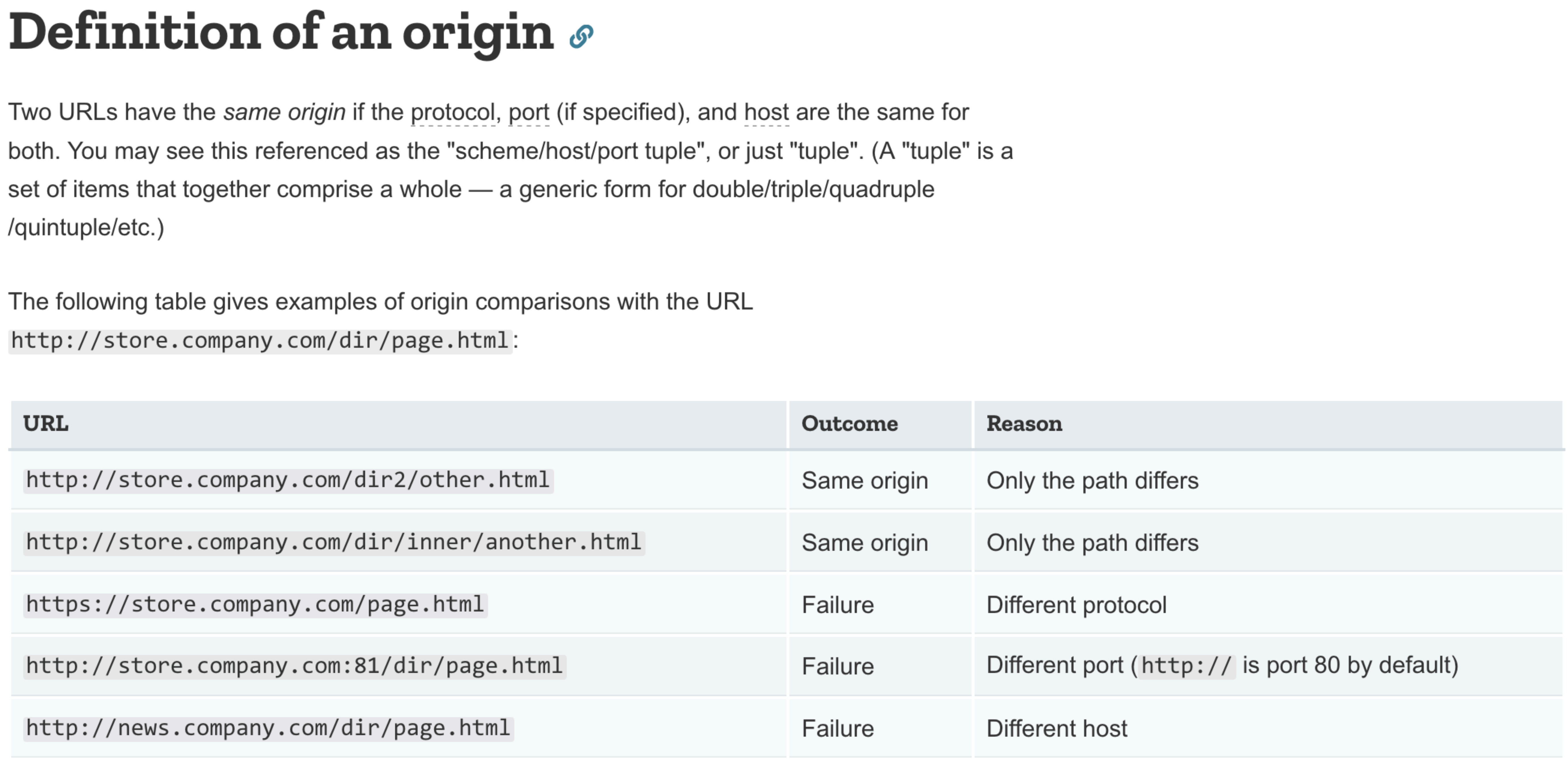
- Steal data from other origins

https://speakerdeck.com/groovecoder/top-5-security-errors-we-see-from-firefox-and-how-to-fix-them

Same-origin Policy blocking a Cross-Origin Request



```
⚠ Cross-Origin Request Blocked: The Same Origin Policy disallows reading the remote resource at https://public.slidesharecdn.com/fonts
  /fontawesome-webfont.woff2?97493d3f11. (Reason: CORS header ‘Access-Control-Allow-Origin’ missing). [Learn More]
```



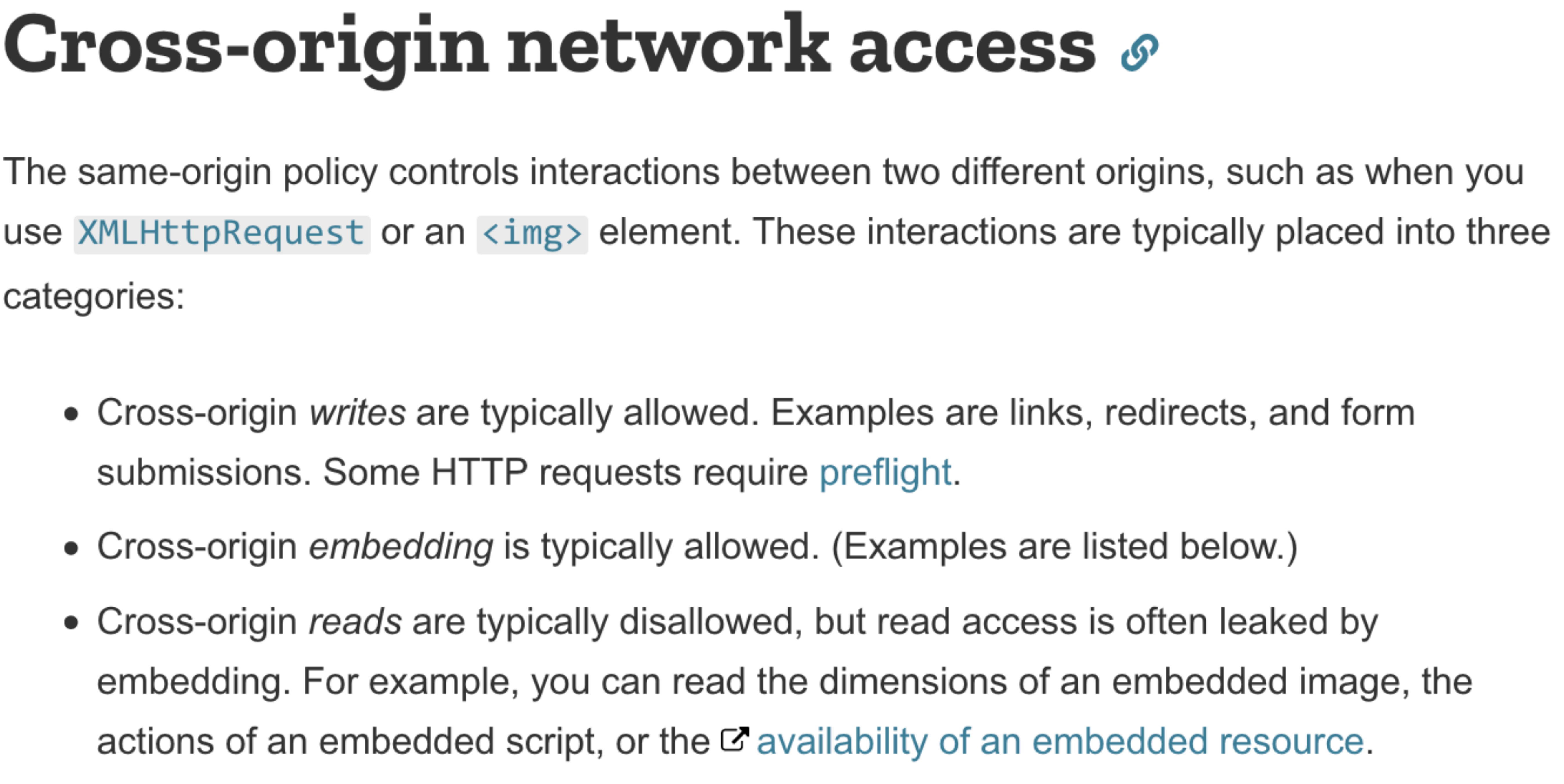
Definition of an origin

Two URLs have the *same origin* if the protocol, port (if specified), and host are the same for both. You may see this referenced as the "scheme/host/port tuple", or just "tuple". (A "tuple" is a set of items that together comprise a whole — a generic form for double/triple/quadruple /quintuple/etc.)

The following table gives examples of origin comparisons with the URL `http://store.company.com/dir/page.html`:

URL	Outcome	Reason
`http://store.company.com/dir2/other.html`	Same origin	Only the path differs
`http://store.company.com/dir/inner/another.html`	Same origin	Only the path differs
`https://store.company.com/page.html`	Failure	Different protocol
`http://store.company.com:81/dir/page.html`	Failure	Different port (`http://` is port 80 by default)
`http://news.company.com/dir/page.html`	Failure	Different host

https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy#Definition_of_an_origin



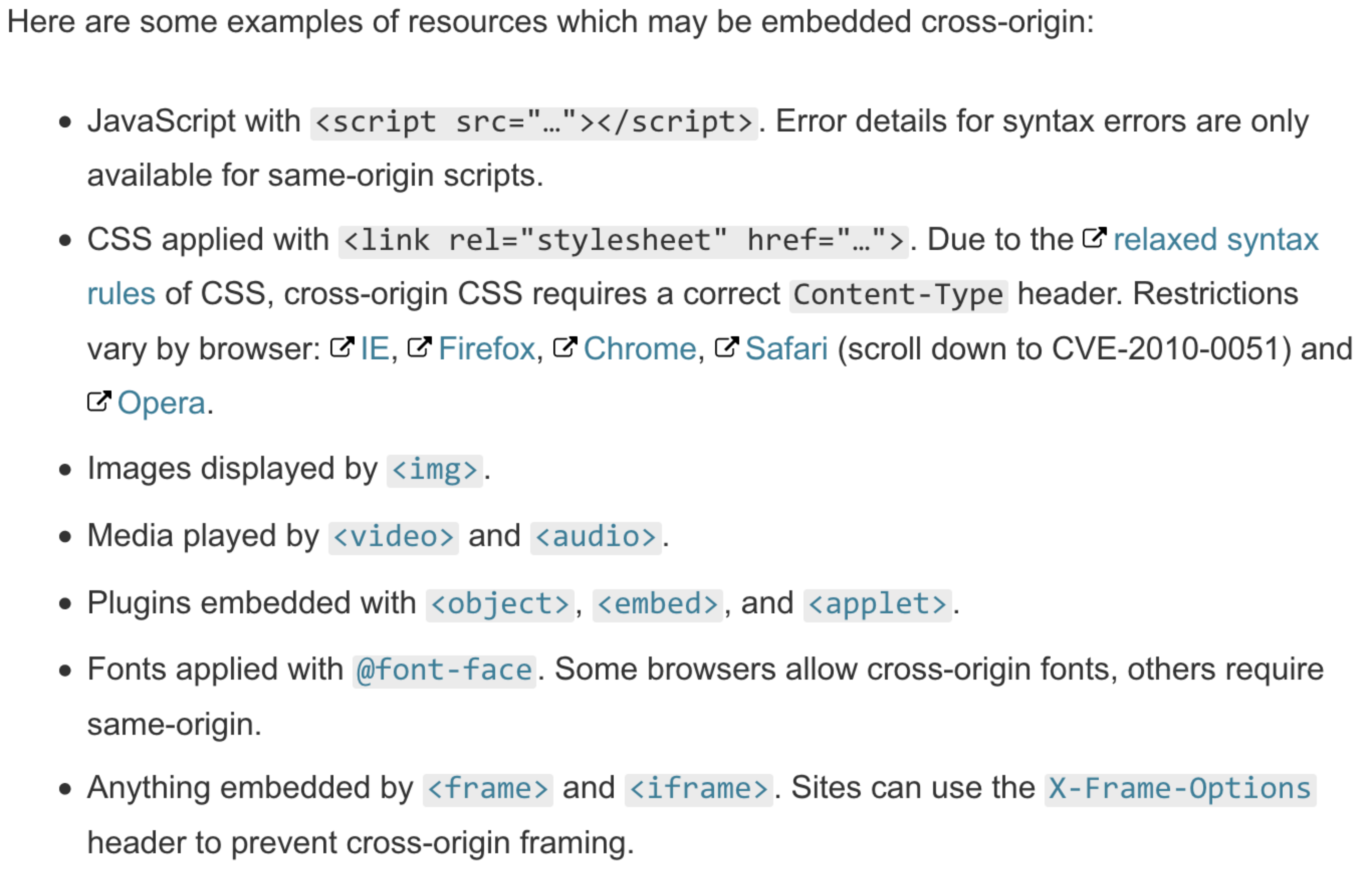
Cross-origin network access

The same-origin policy controls interactions between two different origins, such as when you use `XMLHttpRequest` or an `<img>` element. These interactions are typically placed into three categories:

- Cross-origin *writes* are typically allowed. Examples are links, redirects, and form submissions. Some HTTP requests require preflight.
- Cross-origin *embedding* is typically allowed. (Examples are listed below.)
- Cross-origin *reads* are typically disallowed, but read access is often leaked by embedding. For example, you can read the dimensions of an embedded image, the actions of an embedded script, or the availability of an embedded resource.

https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy#Cross-origin_network_access

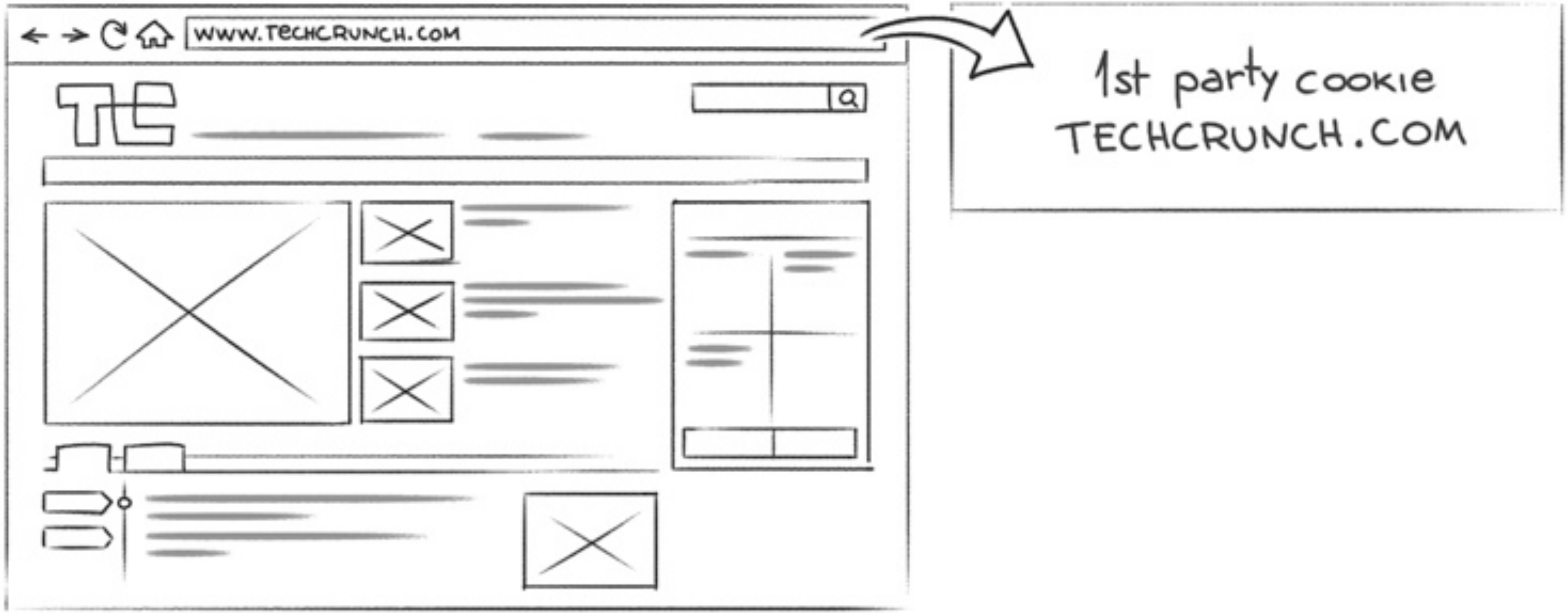
Embedding Resources from other Origins



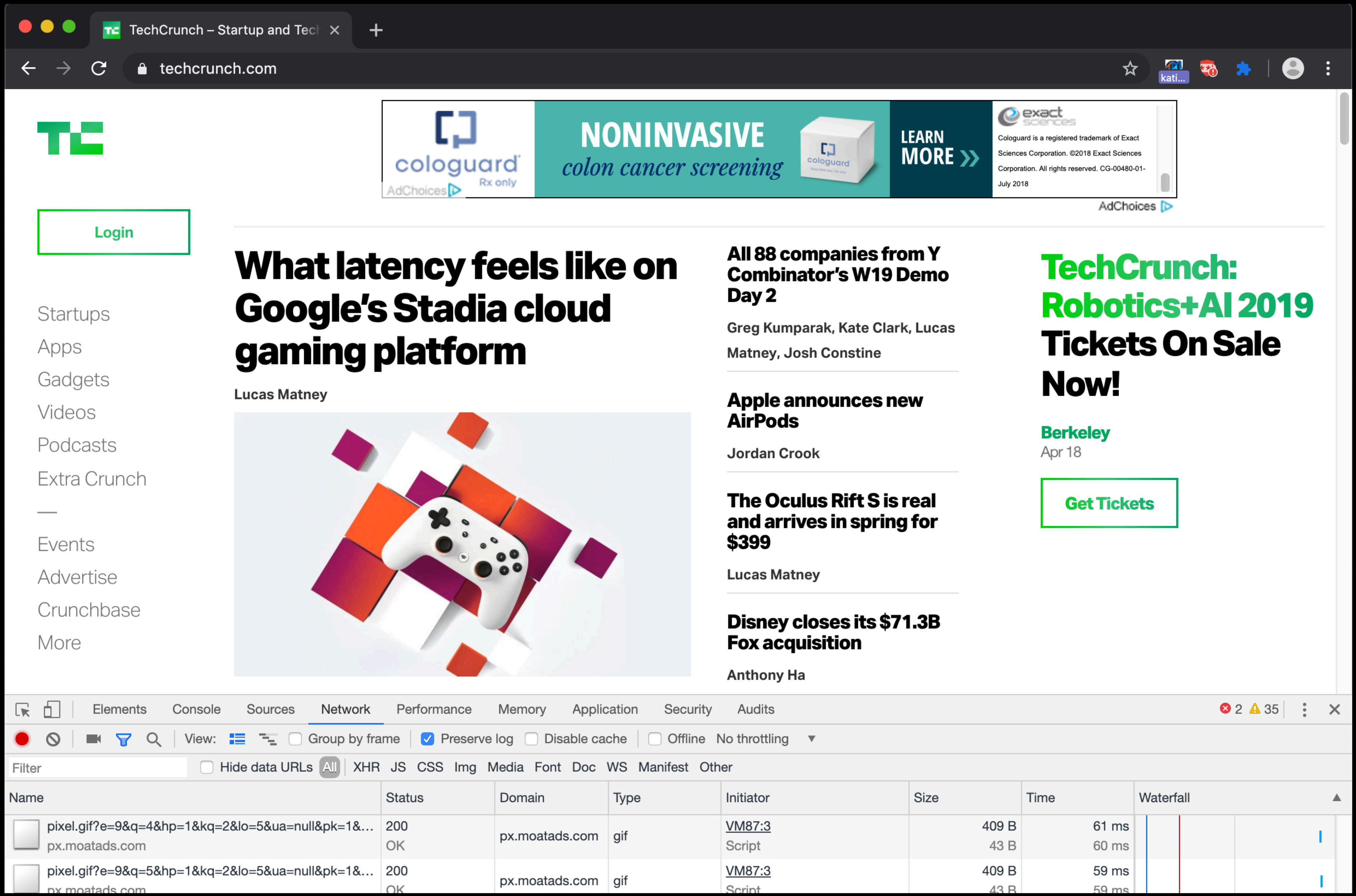
Here are some examples of resources which may be embedded cross-origin:

- JavaScript with `<script src="…"></script>`. Error details for syntax errors are only available for same-origin scripts.
- CSS applied with `<link rel="stylesheet" href="…">`. Due to the relaxed syntax rules of CSS, cross-origin CSS requires a correct `Content-Type` header. Restrictions vary by browser: IE, Firefox, Chrome, Safari (scroll down to CVE-2010-0051) and Opera.
- Images displayed by `<img>`.
- Media played by `<video>` and `<audio>`.
- Plugins embedded with `<object>`, `<embed>`, and `<applet>`.
- Fonts applied with `@font-face`. Some browsers allow cross-origin fonts, others require same-origin.
- Anything embedded by `<frame>` and `<iframe>`. Sites can use the `X-Frame-Options` header to prevent cross-origin framing.

https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy#Cross-origin_network_access



http://clearcode.cc/2015/12/cookie-syncing/



What latency feels like on Google's Stadia cloud gaming platform

Lucas Matney

All 88 companies from Y Combinator's W19 Demo Day 2

Greg Kumparak, Kate Clark, Lucas Matney, Josh Constine

Apple announces new AirPods

Jordan Crook

The Oculus Rift S is real and arrives in spring for $399

Lucas Matney

Disney closes its $71.3B Fox acquisition

Anthony Ha

TechCrunch: Robotics+AI 2019 Tickets On Sale Now!

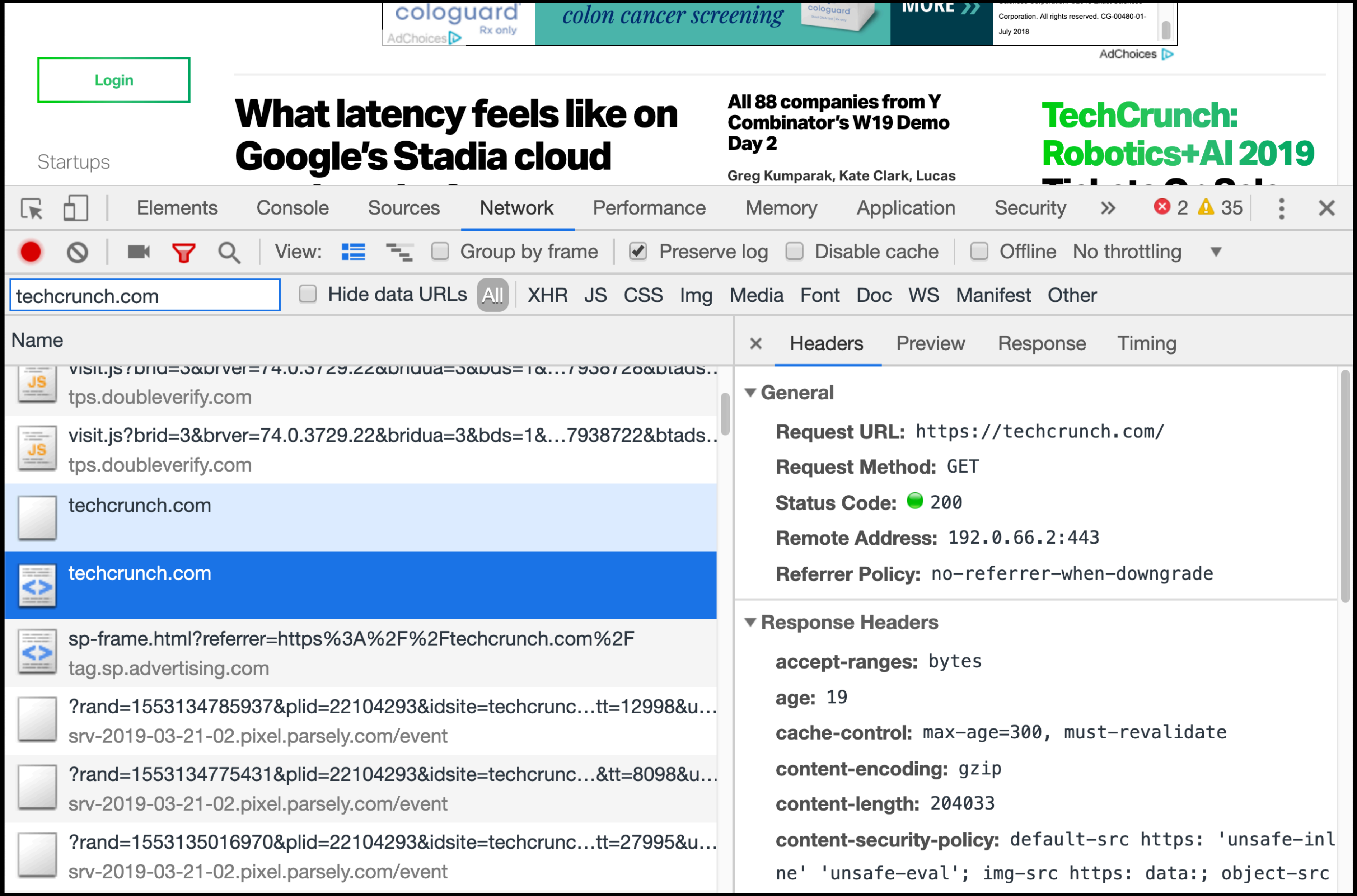
Berkeley
Apr 18

□ Group by frame ☑ Preserve log □ Disable cache □ Offline No throttling

□ Hide data URLs

Name	Status	Domain	Type	Initiator	Size	Time
pixel.gif?e=9&q=4&hp=1&kq=2&lo=5&ua=null&pk=1&... px.moatads.com	200 OK	px.moatads.com	gif	VM87:3 Script	409 B 43 B	61 ms 60 ms
pixel.gif?e=9&q=5&hp=1&kq=2&lo=5&ua=null&pk=1&... px.moatads.com	200 OK	px.moatads.com	gif	VM87:3 Script	409 B 43 B	59 ms 59 ms

600 HTTP requests



What latency feels like on Google's Stadia cloud

All 88 companies from Y Combinator's W19 Demo Day 2

Greg Kumparak, Kate Clark, Lucas

TechCrunch: Robotics+AI 2019

□ Group by frame ☑ Preserve log □ Disable cache □ Offline No throttling

Filter: techcrunch.com

```
visit.js?brid=3&brver=74.0.3729.22&bridua=3&bds=1&…7938722&btads..
tps.doubleverify.com
visit.js?brid=3&brver=74.0.3729.22&bridua=3&bds=1&…7938722&btads..
tps.doubleverify.com
techcrunch.com
techcrunch.com
sp-frame.html?referrer=https%3A%2F%2Ftechcrunch.com%2F
tag.sp.advertising.com
?rand=1553134785937&plid=22104293&idsite=techcrunc…tt=12998&u…
srv-2019-03-21-02.pixel.parsely.com/event
?rand=1553134775431&plid=22104293&idsite=techcrunc…&tt=8098&u…
srv-2019-03-21-02.pixel.parsely.com/event
?rand=1553135016970&plid=22104293&idsite=techcrunc…tt=27995&u…
srv-2019-03-21-02.pixel.parsely.com/event
```

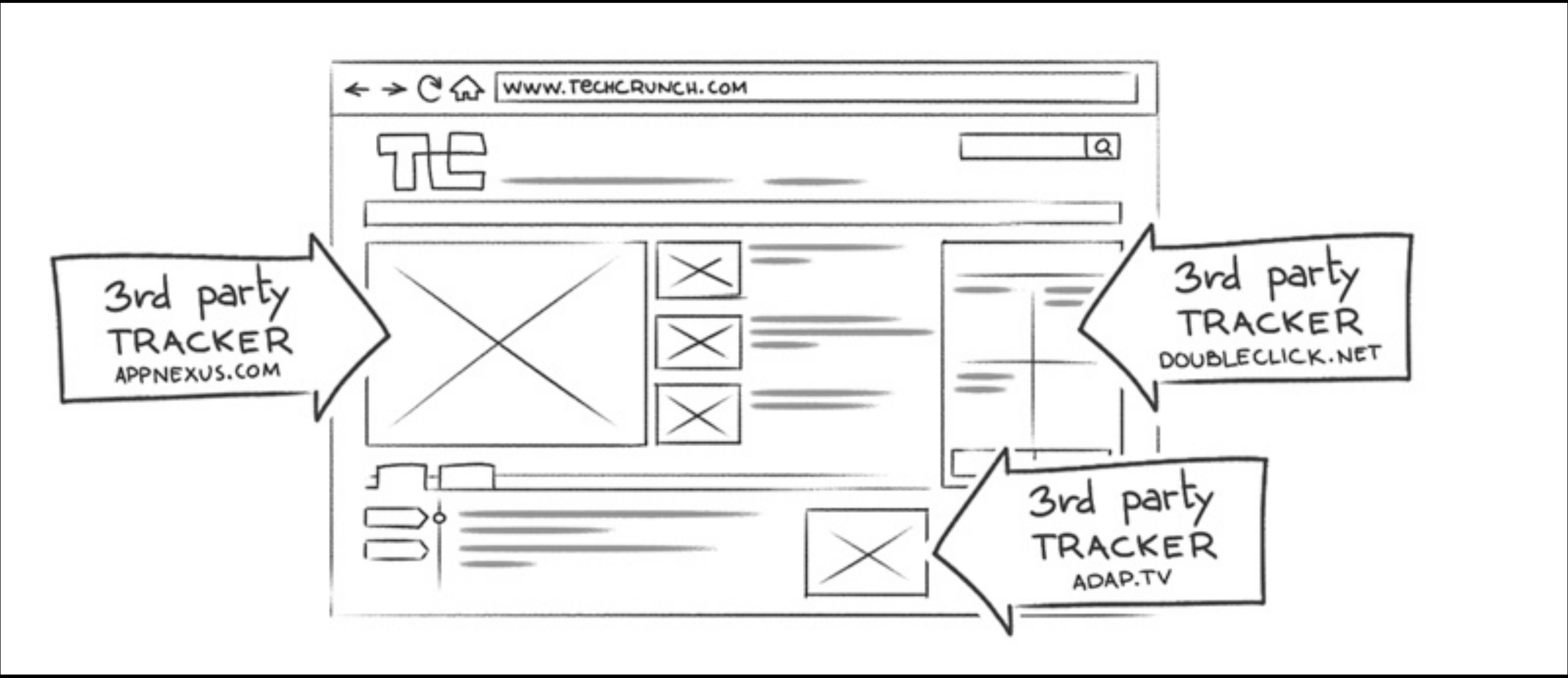
▼ General

```
Request URL: https://techcrunch.com/
Request Method: GET
Status Code: ● 200
Remote Address: 192.0.66.2:443
Referrer Policy: no-referrer-when-downgrade
```

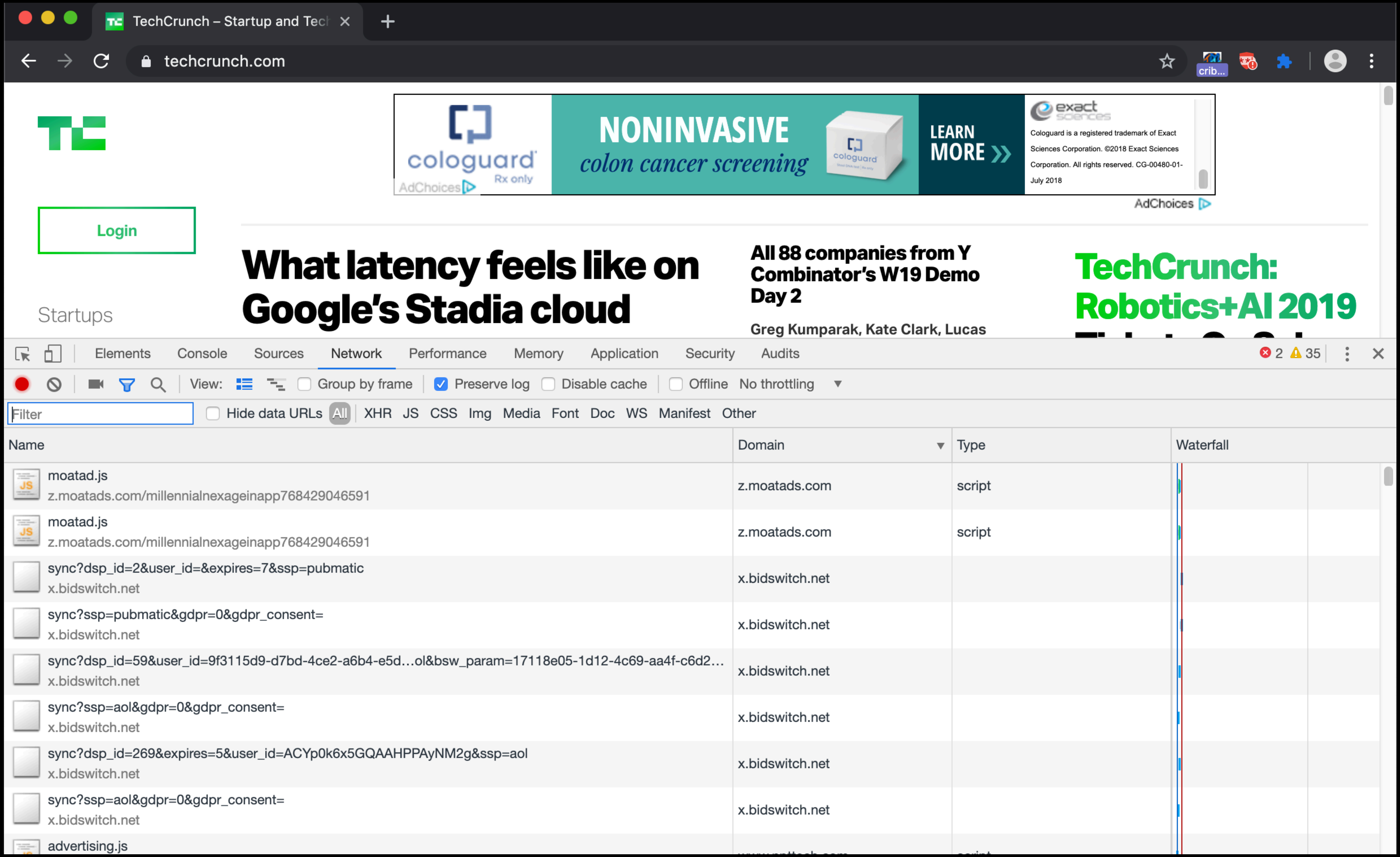
▼ Response Headers

```
accept-ranges: bytes
age: 19
cache-control: max-age=300, must-revalidate
content-encoding: gzip
content-length: 204033
content-security-policy: default-src https: 'unsafe-inl
ne' 'unsafe-eval'; img-src https: data:; object-src
```

53 HTTP requests to techcrunch.com


WWW.TECHCRUNCH.COM
TC
3rd party TRACKER APPNEXUS.COM
3rd party TRACKER DOUBLECLICK.NET
3rd party TRACKER ADAP.TV

http://clearcode.cc/2015/12/cookie-syncing/



What latency feels like on Google's Stadia cloud

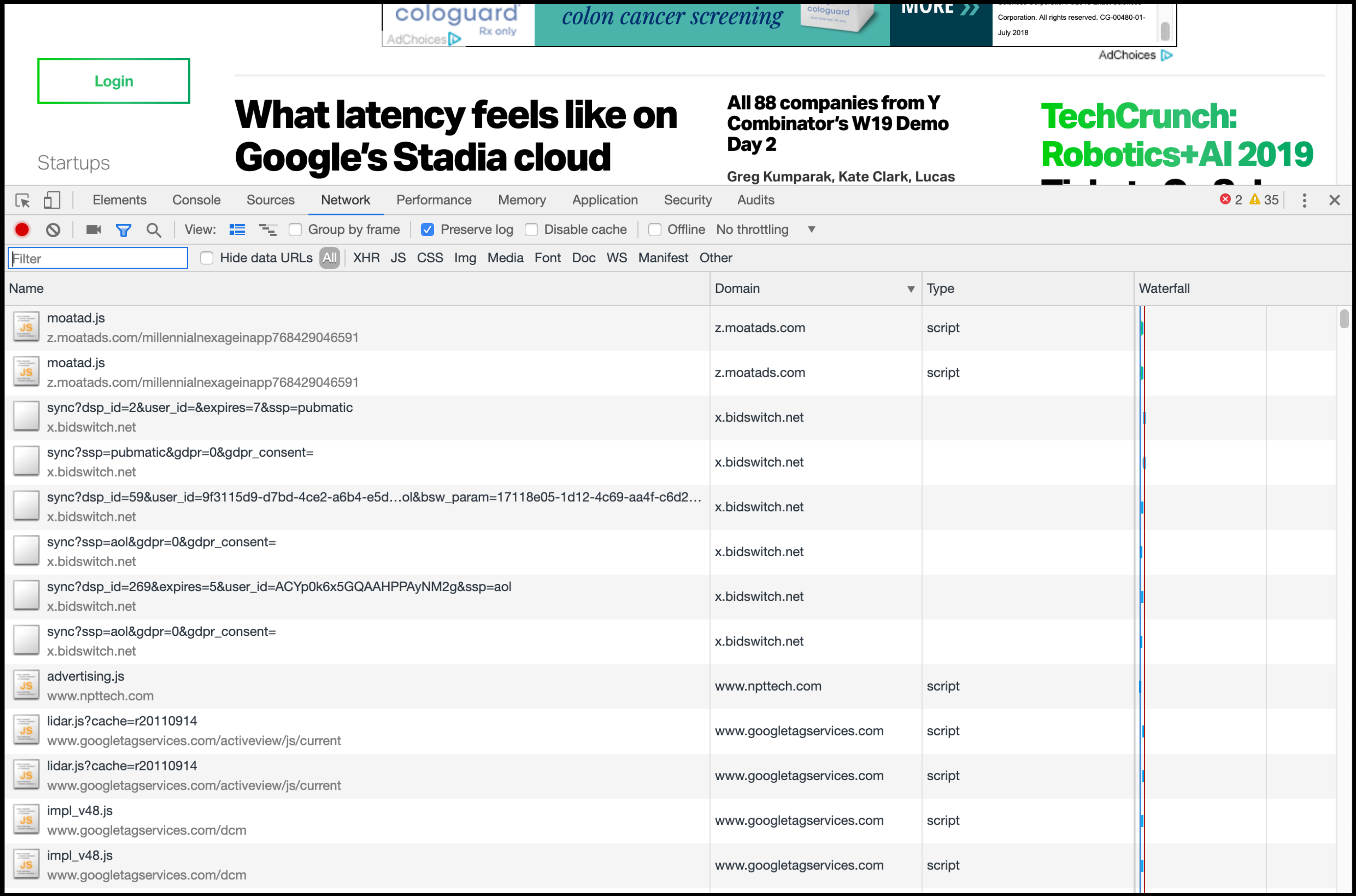
All 88 companies from Y Combinator's W19 Demo Day 2

Greg Kumparak, Kate Clark, Lucas

TechCrunch: Robotics+AI 2019

Name	Domain	Type	Waterfall
moatad.js z.moatads.com/millennialnexageinapp768429046591	z.moatads.com	script	
moatad.js z.moatads.com/millennialnexageinapp768429046591	z.moatads.com	script	
sync?dsp_id=2&user_id=&expires=7&ssp=pubmatic x.bidswitch.net	x.bidswitch.net		
sync?ssp=pubmatic&gdpr=0&gdpr_consent= x.bidswitch.net	x.bidswitch.net		
sync?dsp_id=59&user_id=9f3115d9-d7bd-4ce2-a6b4-e5d…ol&bsw_param=17118e05-1d12-4c69-aa4f-c6d2… x.bidswitch.net	x.bidswitch.net		
sync?ssp=aol&gdpr=0&gdpr_consent= x.bidswitch.net	x.bidswitch.net		
sync?dsp_id=269&expires=5&user_id=ACYp0k6x5GQAAHPPAyNM2g&ssp=aol x.bidswitch.net	x.bidswitch.net		
sync?ssp=aol&gdpr=0&gdpr_consent= x.bidswitch.net	x.bidswitch.net		
advertising.js			

547 HTTP requests to other origins



What latency feels like on Google's Stadia cloud

All 88 companies from Y Combinator's W19 Demo Day 2

Greg Kumparak, Kate Clark, Lucas

TechCrunch: Robotics+AI 2019

□ Group by frame ☑ Preserve log □ Disable cache □ Offline No throttling

□ Hide data URLs

Name	Domain	Type	Waterfall
moatad.js z.moatads.com/millennialnexageinapp768429046591	z.moatads.com	script	
moatad.js z.moatads.com/millennialnexageinapp768429046591	z.moatads.com	script	
sync?dsp_id=2&user_id=&expires=7&ssp=pubmatic x.bidswitch.net	x.bidswitch.net		
sync?ssp=pubmatic&gdpr=0&gdpr_consent= x.bidswitch.net	x.bidswitch.net		
sync?dsp_id=59&user_id=9f3115d9-d7bd-4ce2-a6b4-e5d…ol&bsw_param=17118e05-1d12-4c69-aa4f-c6d2… x.bidswitch.net	x.bidswitch.net		
sync?ssp=aol&gdpr=0&gdpr_consent= x.bidswitch.net	x.bidswitch.net		
sync?dsp_id=269&expires=5&user_id=ACYp0k6x5GQAAHPPAyNM2g&ssp=aol x.bidswitch.net	x.bidswitch.net		
sync?ssp=aol&gdpr=0&gdpr_consent= x.bidswitch.net	x.bidswitch.net		
advertising.js www.npttech.com	www.npttech.com	script	
lidar.js?cache=r20110914 www.googletagservices.com/activeview/js/current	www.googletagservices.com	script	
lidar.js?cache=r20110914 www.googletagservices.com/activeview/js/current	www.googletagservices.com	script	
impl_v48.js www.googletagservices.com/dcm	www.googletagservices.com	script	
impl_v48.js www.googletagservices.com/dcm	www.googletagservices.com	script	

547 HTTP requests to other origins

Google, Facebook, Yahoo, DoubleClick, DoubleVerify, advertising.com, parsely.com, scorecardresearch.com, moatads.com, wp.com, typekit.net, betrad.com, cloudfront.net, nr-data.net, atwola.com, bidswitch.net, npttech.com, krxd.net, simpli.fi, taboola.com, pswec.com, mathtag.com, ipredictive.com, 1rx.io, everesttech.net, casalemedia.com, pubmatic.com, adnxs.com, 2mdn.net, yimg.com, adentifi.com, gwallet.com, owneriq.net, adhigh.net, netmng.com, …

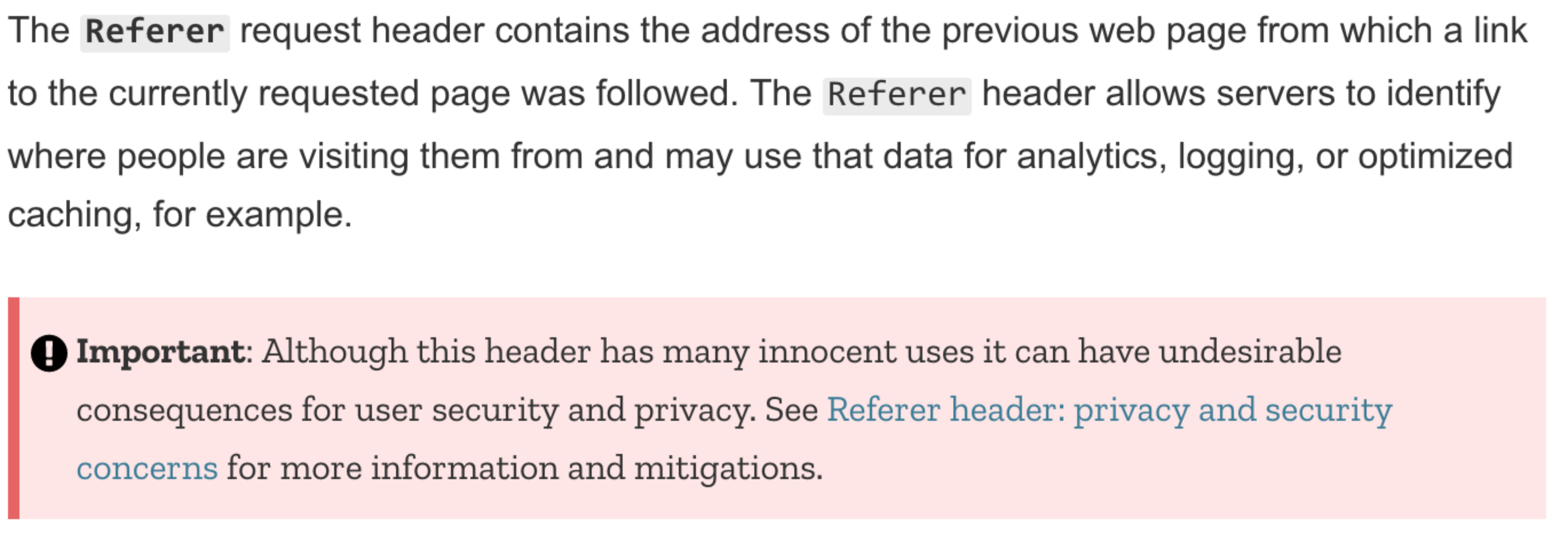
Embedded Cross-Origin Requests

```
http://techcrunch.com

<html>
 …
   <script src=“https://connect.facebook.net/
en_US/fbevents.js"></script>
   <iframe src=“https://
googleads.g.doubleclick.net/xbbe/match?
rmxinit=1&xid=7JwNU2U1TE1_TTIc6ggpZi3A"></
iframe>
 …
</html>
```

https://speakerdeck.com/groovecoder/top-5-security-errors-we-see-from-firefox-and-how-to-fix-them

Embedded Cross-Origin Requests include `Referers`

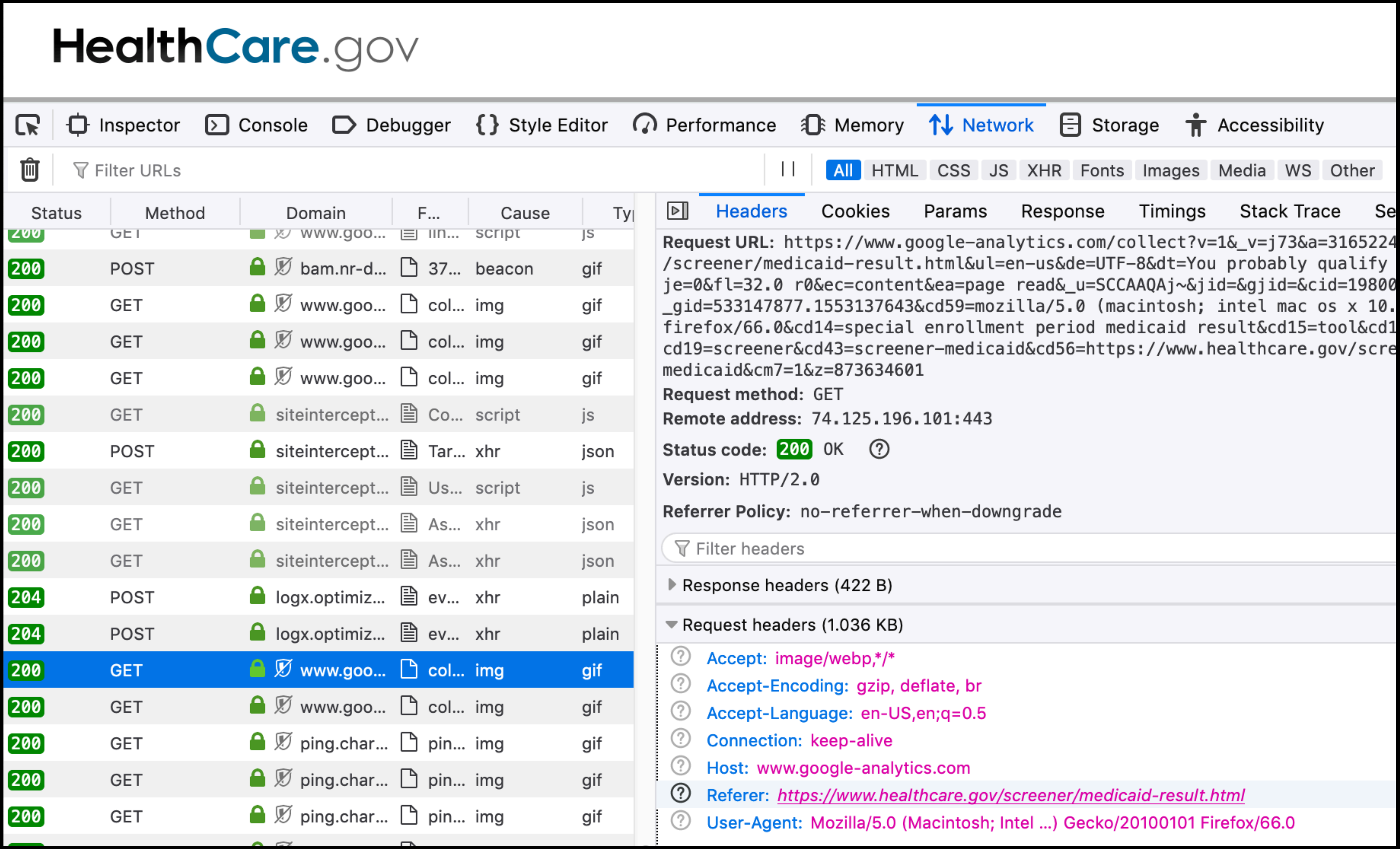
Referers [sic]



The `Referer` request header contains the address of the previous web page from which a link to the currently requested page was followed. The `Referer` header allows servers to identify where people are visiting them from and may use that data for analytics, logging, or optimized caching, for example.

❗ **Important**: Although this header has many innocent uses it can have undesirable consequences for user security and privacy. See Referer header: privacy and security concerns for more information and mitigations.

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referer



Status	Method	Domain	F...	Cause	Ty
200	GET	www.goo...	lin...	script	js
200	POST	bam.nr-d...	37...	beacon	gif
200	GET	www.goo...	col...	img	gif
200	GET	www.goo...	col...	img	gif
200	GET	www.goo...	col...	img	gif
200	GET	siteintercept...	Co...	script	js
200	POST	siteintercept...	Tar...	xhr	json
200	GET	siteintercept...	Us...	script	js
200	GET	siteintercept...	As...	xhr	json
200	GET	siteintercept...	As...	xhr	json
204	POST	logx.optimiz...	ev...	xhr	plain
204	POST	logx.optimiz...	ev...	xhr	plain
200	GET	www.goo...	col...	img	gif
200	GET	www.goo...	col...	img	gif
200	GET	ping.char...	pin...	img	gif
200	GET	ping.char...	pin...	img	gif
200	GET	ping.char...	pin...	img	gif

Request URL: https://www.google-analytics.com/collect?v=1&_v=j73&a=3165224
/screener/medicaid-result.html&ul=en-us&de=UTF-8&dt=You probably qualify
je=0&fl=32.0 r0&ec=content&ea=page read&_u=SCCAAQAj~&jid=&gjid=&cid=19800
_gid=533147877.1553137643&cd59=mozilla/5.0 (macintosh; intel mac os x 10.
firefox/66.0&cd14=special enrollment period medicaid result&cd15=tool&cd1
cd19=screener&cd43=screener-medicaid&cd56=https://www.healthcare.gov/scre
medicaid&cm7=1&z=873634601

Request method: GET

Remote address: 74.125.196.101:443

Status code: 200 OK

Version: HTTP/2.0

Referrer Policy: no-referrer-when-downgrade

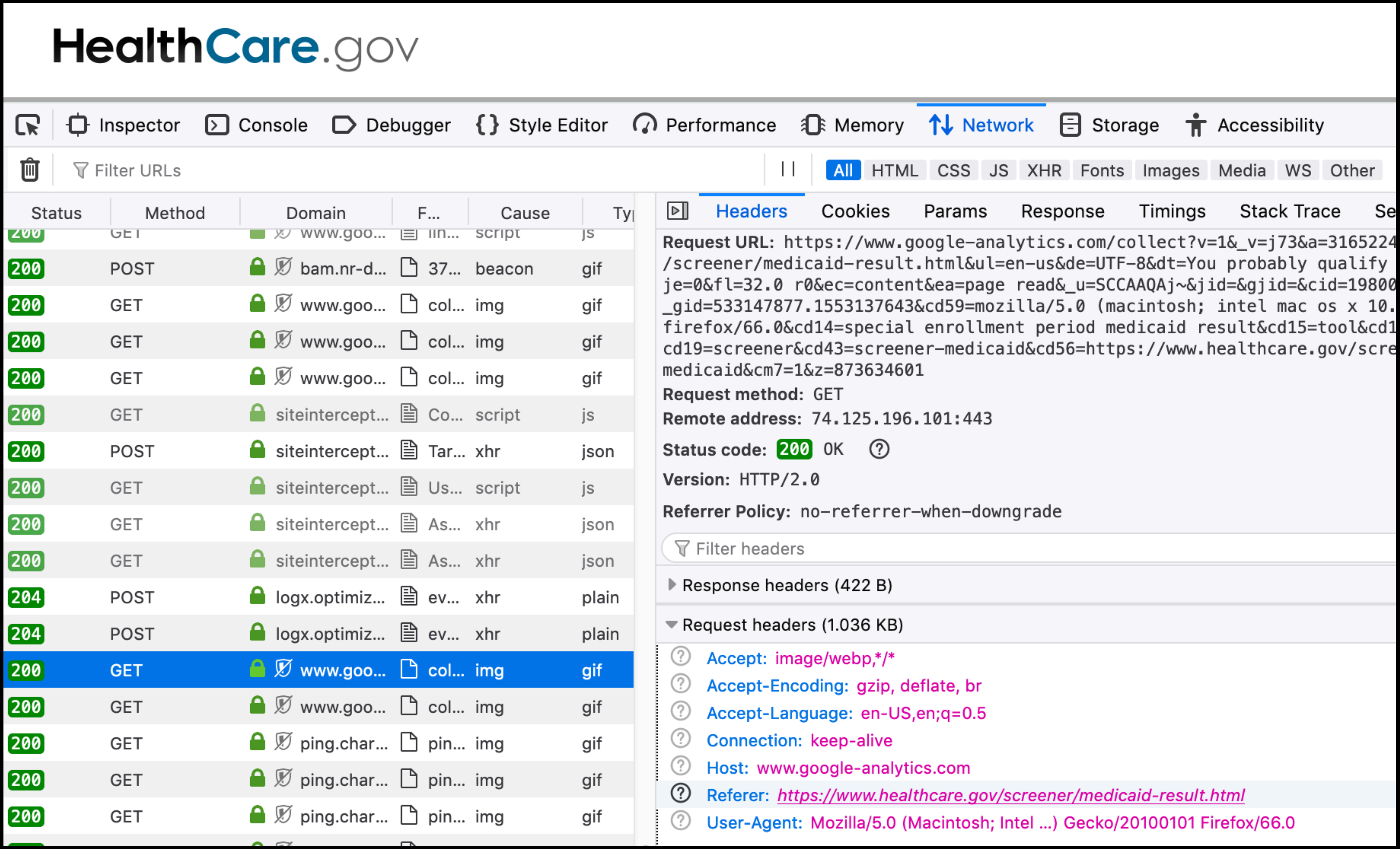
▸ Response headers (422 B)

▾ Request headers (1.036 KB)

Accept: image/webp,*/*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Host: www.google-analytics.com
Referer: *https://www.healthcare.gov/screener/medicaid-result.html*
User-Agent: Mozilla/5.0 (Macintosh; Intel ...) Gecko/20100101 Firefox/66.0

`Referer` tells Google exact page I'm looking at: https://www.healthcare.gov/screener/medicaid-result.html

Note: in reality, most trackers don’t rely on `Referer`



Status	Method	Domain	F...	Cause	Ty
200	GET	www.goo...	lin...	script	js
200	POST	bam.nr-d...	37...	beacon	gif
200	GET	www.goo...	col...	img	gif
200	GET	www.goo...	col...	img	gif
200	GET	www.goo...	col...	img	gif
200	GET	siteintercept...	Co...	script	js
200	POST	siteintercept...	Tar...	xhr	json
200	GET	siteintercept...	Us...	script	js
200	GET	siteintercept...	As...	xhr	json
200	GET	siteintercept...	As...	xhr	json
204	POST	logx.optimiz...	ev...	xhr	plain
204	POST	logx.optimiz...	ev...	xhr	plain
200	GET	www.goo...	col...	img	gif
200	GET	www.goo...	col...	img	gif
200	GET	ping.char...	pin...	img	gif
200	GET	ping.char...	pin...	img	gif
200	GET	ping.char...	pin...	img	gif

Request URL: `https://www.google-analytics.com/collect?v=1&_v=j73&a=3165224`
`/screener/medicaid-result.html&ul=en-us&de=UTF-8&dt=You probably qualify`
`je=0&fl=32.0 r0&ec=content&ea=page read&_u=SCCAAQAj~&jid=&gjid=&cid=19800`
`_gid=533147877.1553137643&cd59=mozilla/5.0 (macintosh; intel mac os x 10.`
`firefox/66.0&cd14=special enrollment period medicaid result&cd15=tool&cd1`
`cd19=screener&cd43=screener-medicaid&cd56=https://www.healthcare.gov/scre`
`medicaid&cm7=1&z=873634601`

Request method: GET

Remote address: 74.125.196.101:443

Status code: 200 OK

Version: HTTP/2.0

Referrer Policy: no-referrer-when-downgrade

▸ Response headers (422 B)

▾ Request headers (1.036 KB)

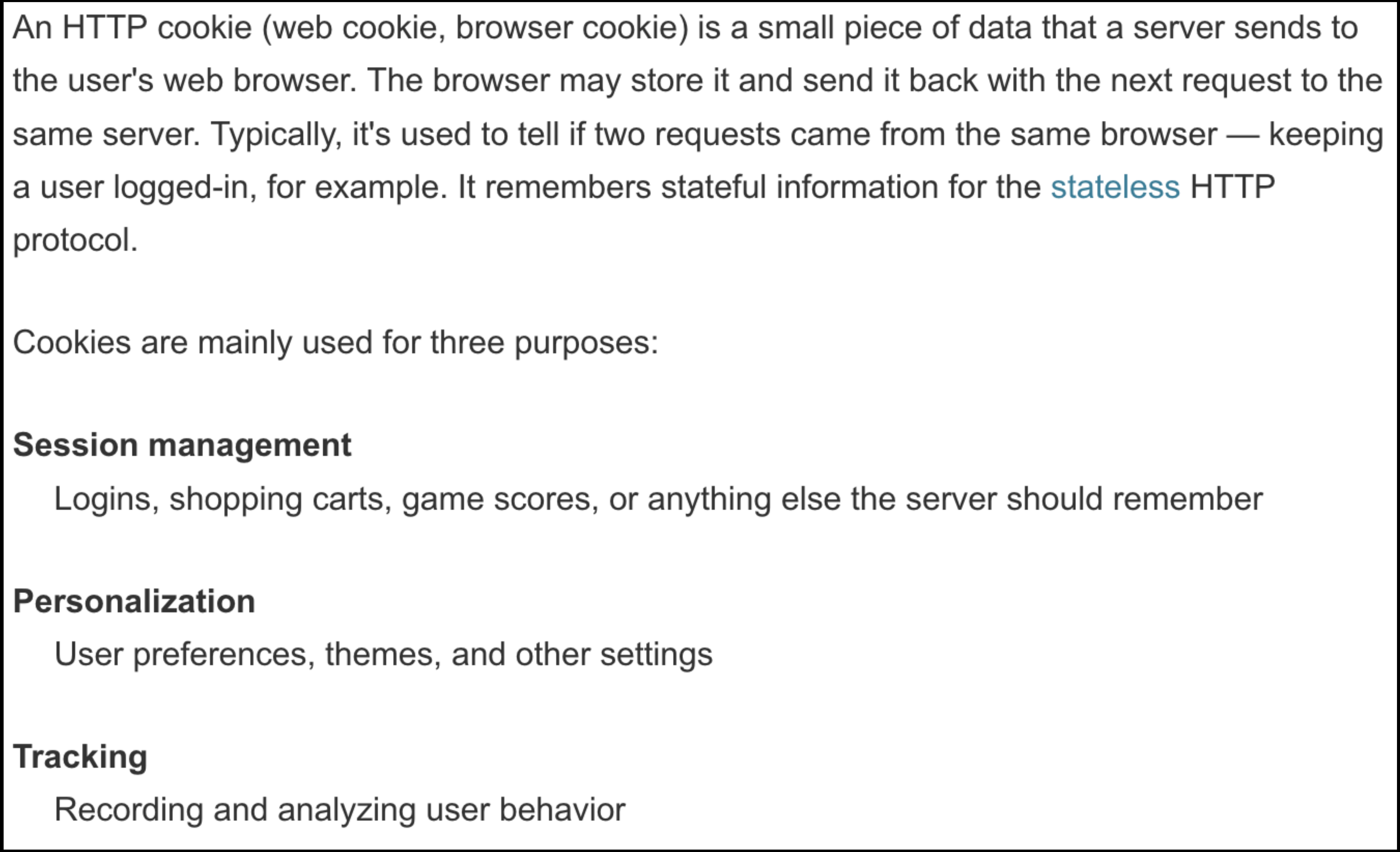
Accept: image/webp,*/*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Host: www.google-analytics.com
Referer: https://www.healthcare.gov/screener/medicaid-result.html
User-Agent: Mozilla/5.0 (Macintosh; Intel ...) Gecko/20100101 Firefox/66.0

Google JS also sends the exact page I’m looking at in a url parameter

Embedded
Cross-Origin Requests
include Cookies

Cookies

Cookies



An HTTP cookie (web cookie, browser cookie) is a small piece of data that a server sends to the user's web browser. The browser may store it and send it back with the next request to the same server. Typically, it's used to tell if two requests came from the same browser — keeping a user logged-in, for example. It remembers stateful information for the stateless HTTP protocol.

Cookies are mainly used for three purposes:

Session management

Logins, shopping carts, game scores, or anything else the server should remember

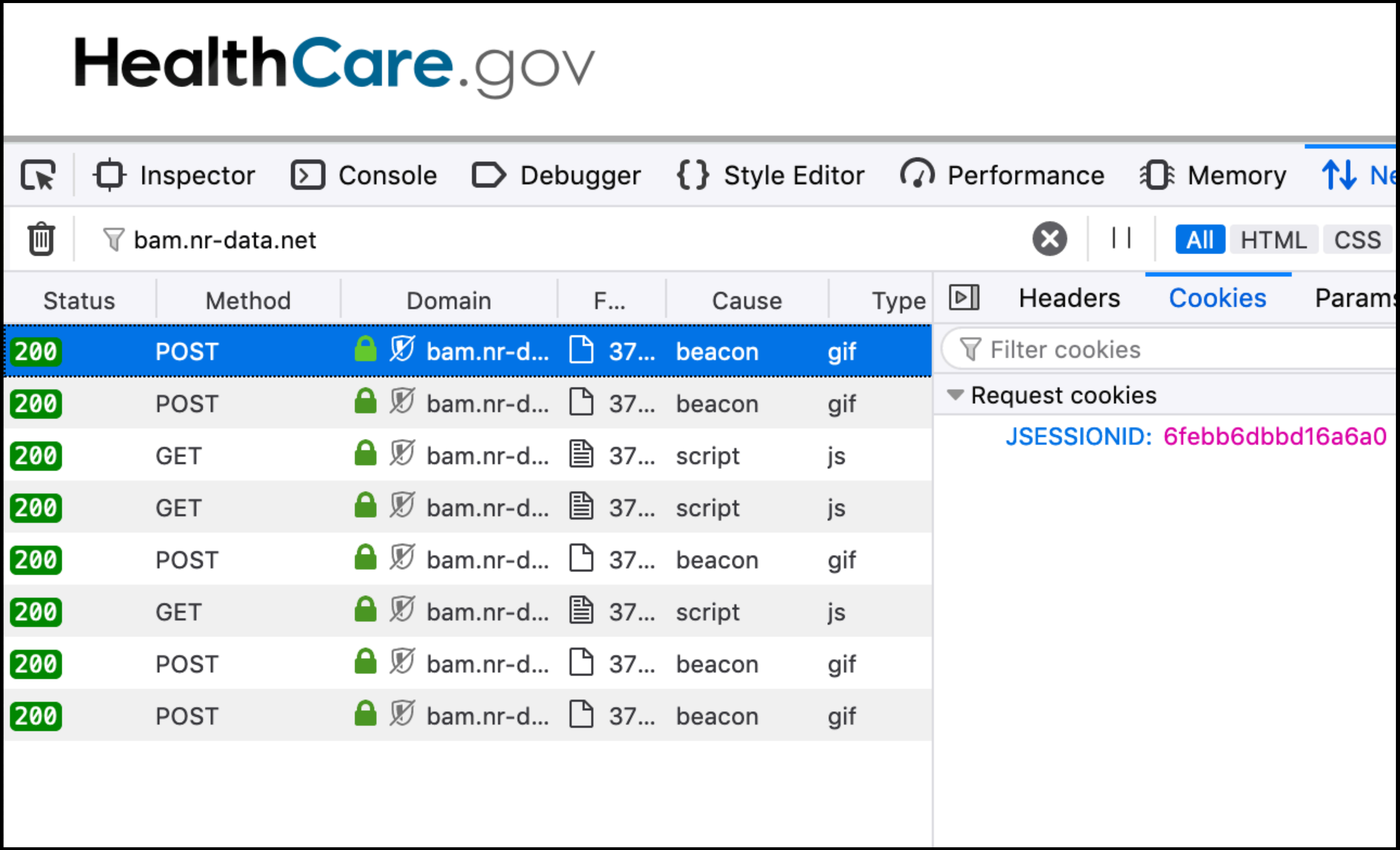
Personalization

User preferences, themes, and other settings

Tracking

Recording and analyzing user behavior

https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies



bam.nr-data.net

Status	Method	Domain	F...	Cause	Type
200	POST	bam.nr-d...	37...	beacon	gif
200	POST	bam.nr-d...	37...	beacon	gif
200	GET	bam.nr-d...	37...	script	js
200	GET	bam.nr-d...	37...	script	js
200	POST	bam.nr-d...	37...	beacon	gif
200	GET	bam.nr-d...	37...	script	js
200	POST	bam.nr-d...	37...	beacon	gif
200	POST	bam.nr-d...	37...	beacon	gif

Request cookies

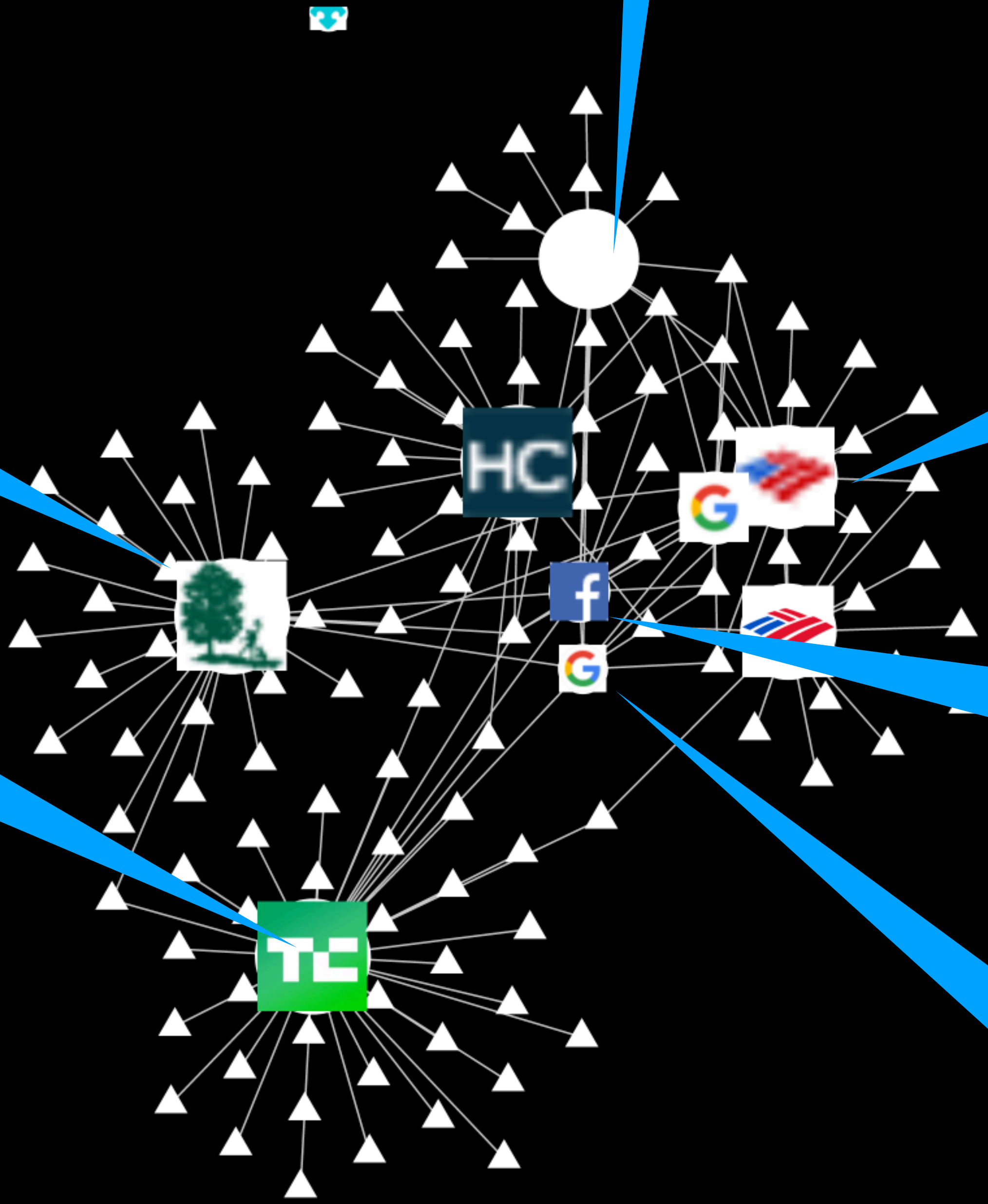
JSESSIONID: 6febb6dbbd16a6a0

Cookies are a persistent identifier for my browser

How tracking works

- “3rd parties”
- visit social-example.com, get cookie
- visit health-example.com, which embeds social-example.com
- social-example.com receives `Cookie` and `Referer` value
- social-example.com builds up a behavior profile

Lightbeam Demo



catholicmom.com

cancercenter.com

bankofamerica.com

techcrunch.com

facebook.com

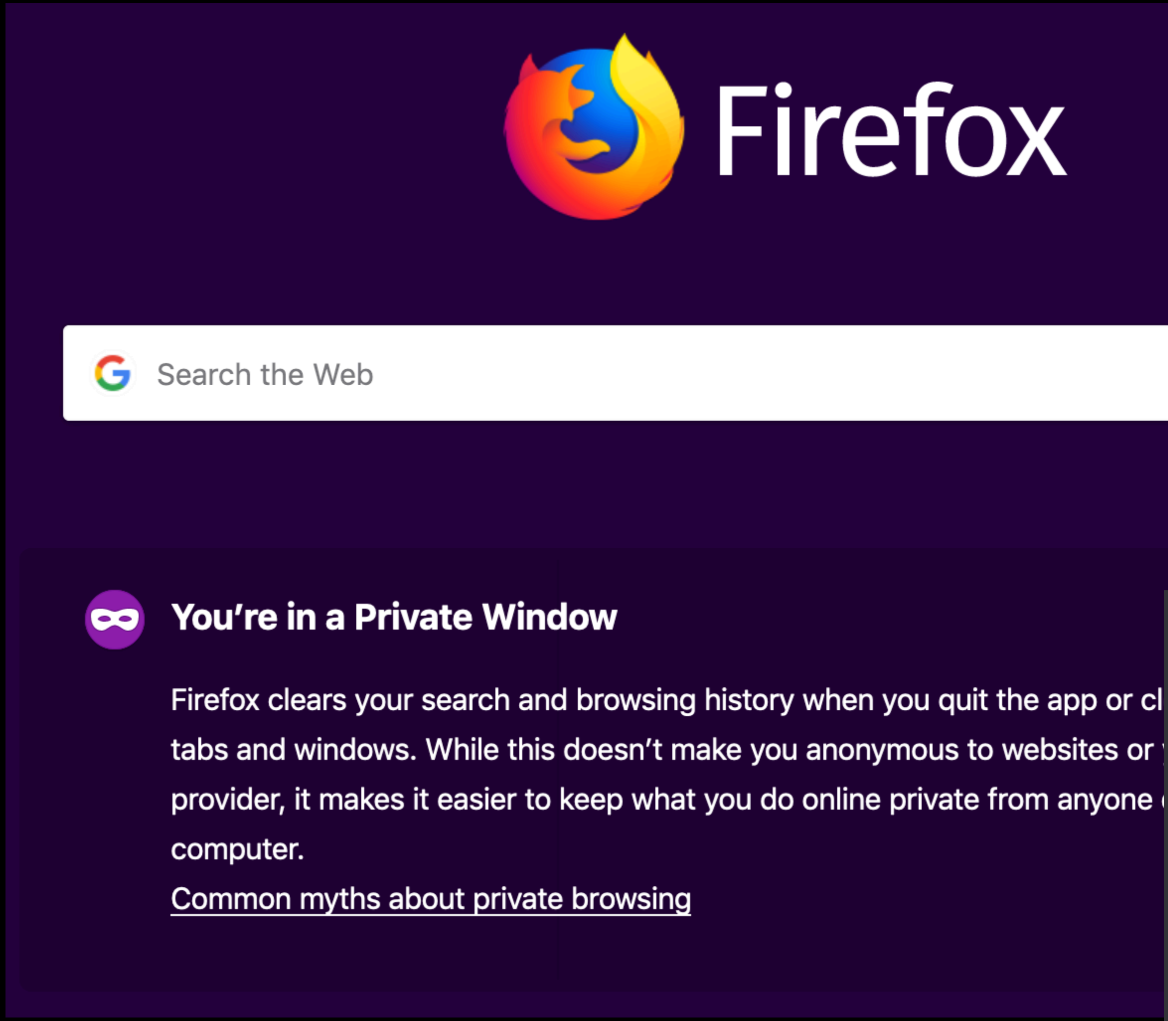
google.com

Privacy Protections built into web browsers

Browser protections

- Clear cookies after every browsing session
- No 3rd-party cookies
    - Except from visited sites (Like Safari ITP)
- Strip paths from `Referers` to 3rd parties
- Tracking Protection (Firefox, Safari, Tor)
- First-Party Isolation (Firefox, Tor)
- Resist Fingerprinting (Firefox, Tor)

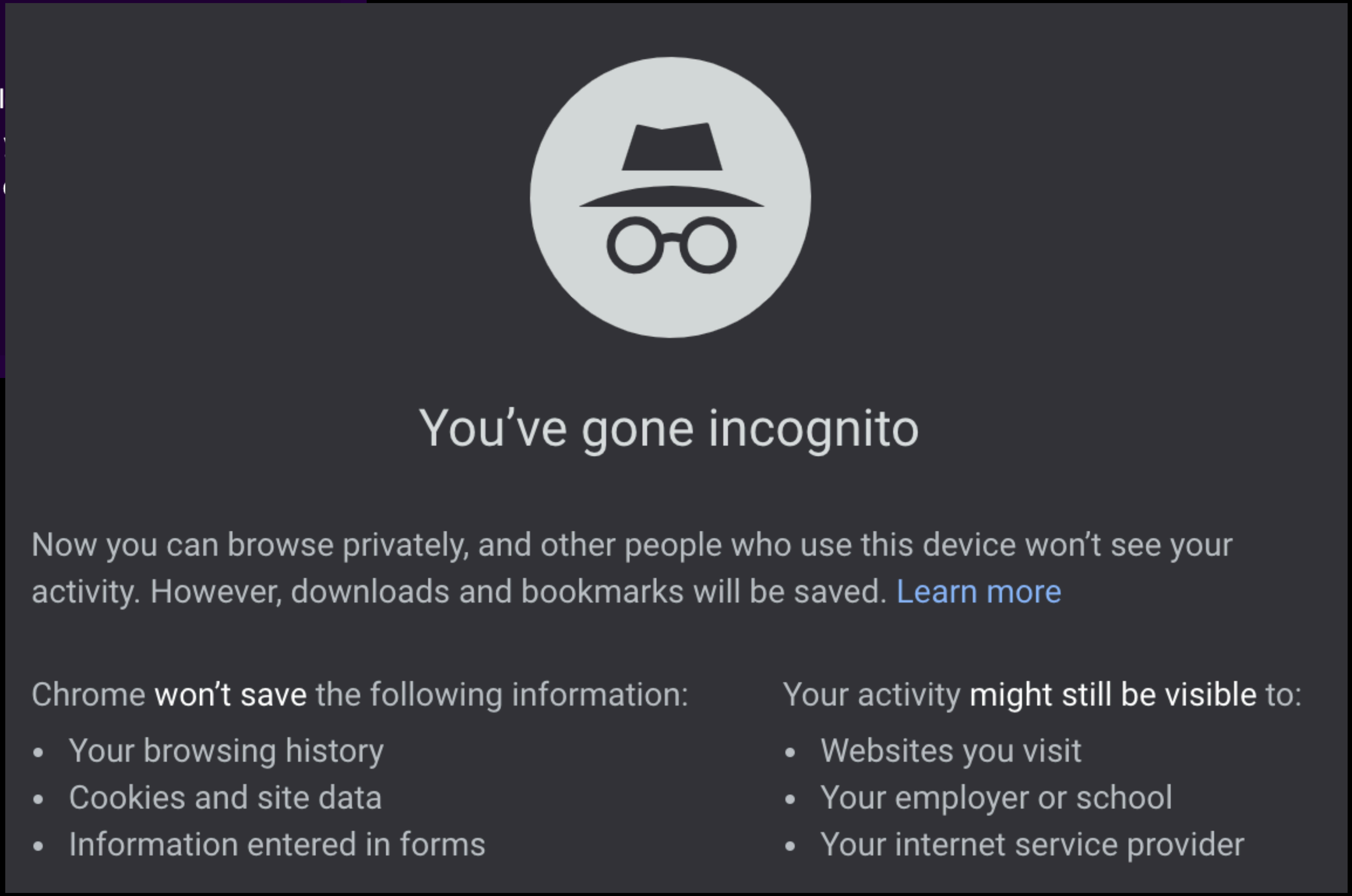
Private/Incognito Browsing



You’re in a Private Window

Firefox clears your search and browsing history when you quit the app or cl
tabs and windows. While this doesn’t make you anonymous to websites or
provider, it makes it easier to keep what you do online private from anyone
computer.

Common myths about private browsing



You’ve gone incognito

Now you can browse privately, and other people who use this device won’t see your activity. However, downloads and bookmarks will be saved. Learn more

Chrome **won’t save** the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

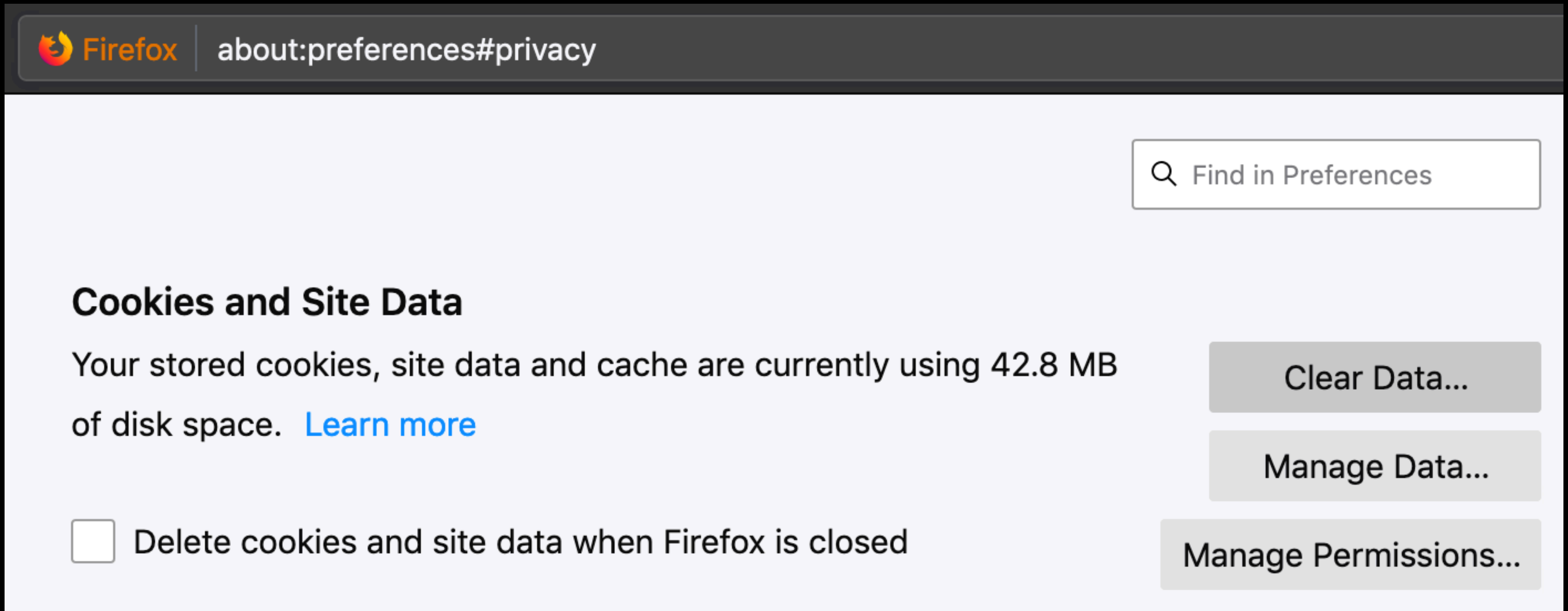
Your activity **might still be visible** to:

- Websites you visit
- Your employer or school
- Your internet service provider

Private/Incognito Browsing

- Designed for local adversaries
- Doesn’t remember search & browsing history
- Doesn’t remember form input
- Clears cookies on exit

Clear your cookies



Firefox about:preferences#privacy

Find in Preferences

Cookies and Site Data

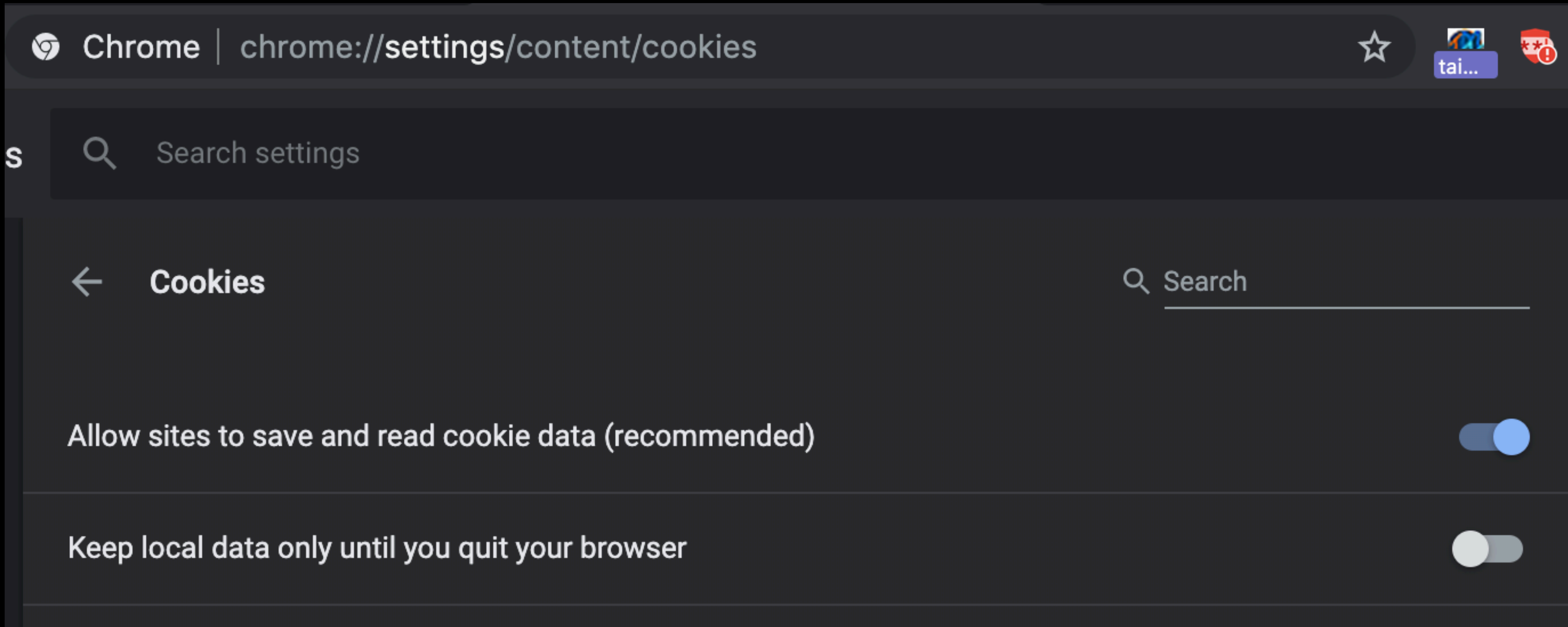
Your stored cookies, site data and cache are currently using 42.8 MB of disk space. Learn more

Clear Data...

Manage Data...

□ Delete cookies and site data when Firefox is closed

Manage Permissions...



Chrome | chrome://settings/content/cookies

Search settings

Cookies

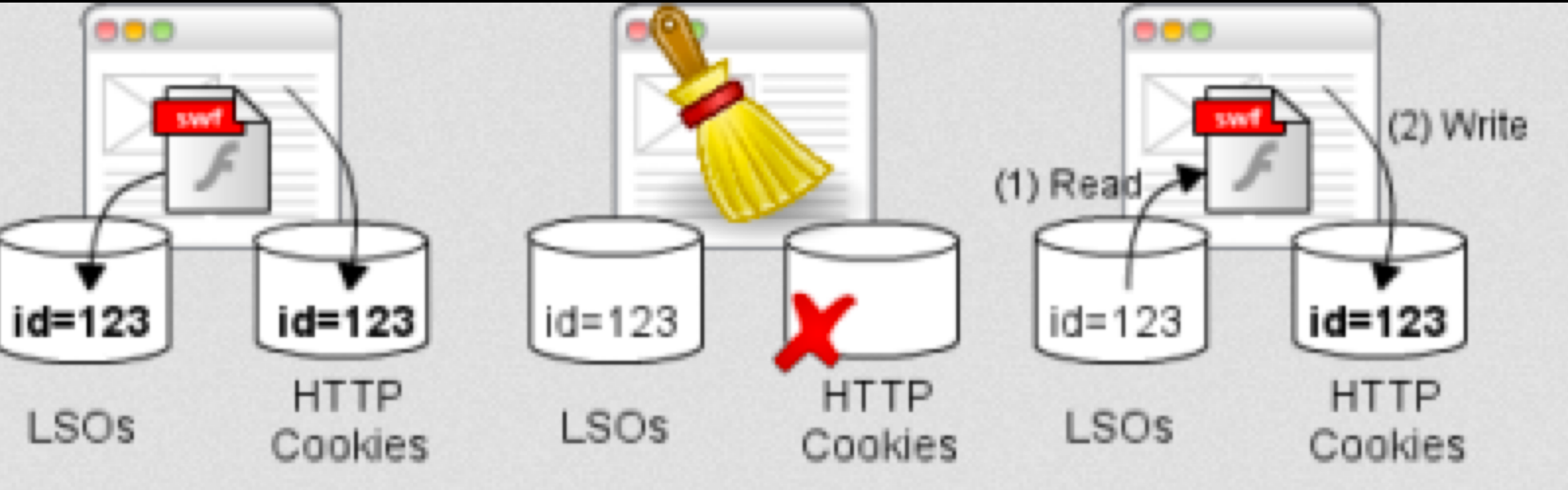
Search

Allow sites to save and read cookie data (recommended) ●

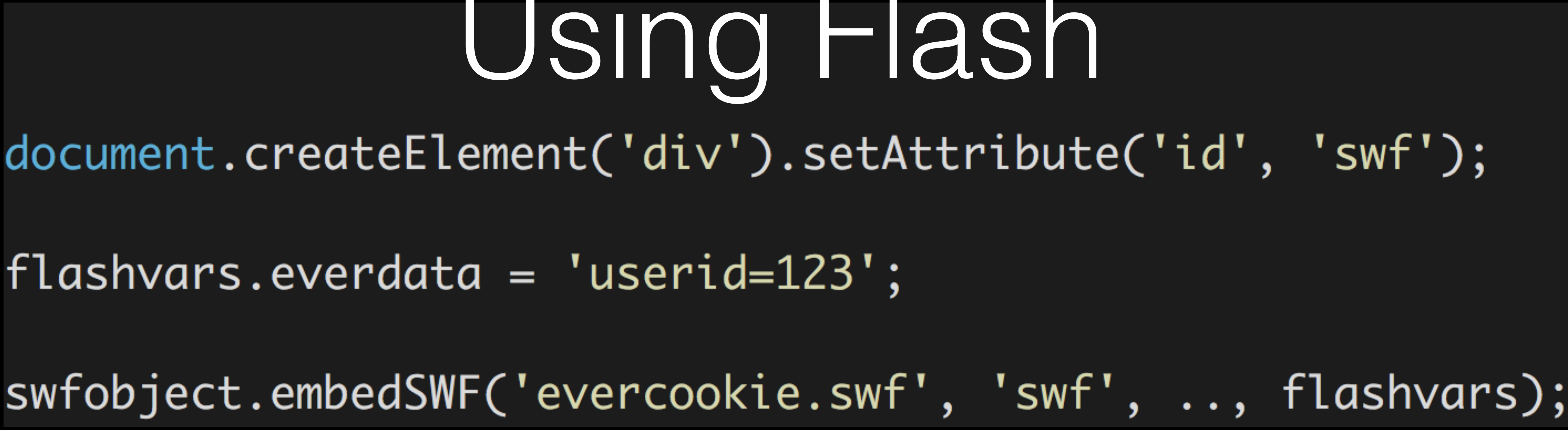
Keep local data only until you quit your browser ○

Cookie Re-spawning

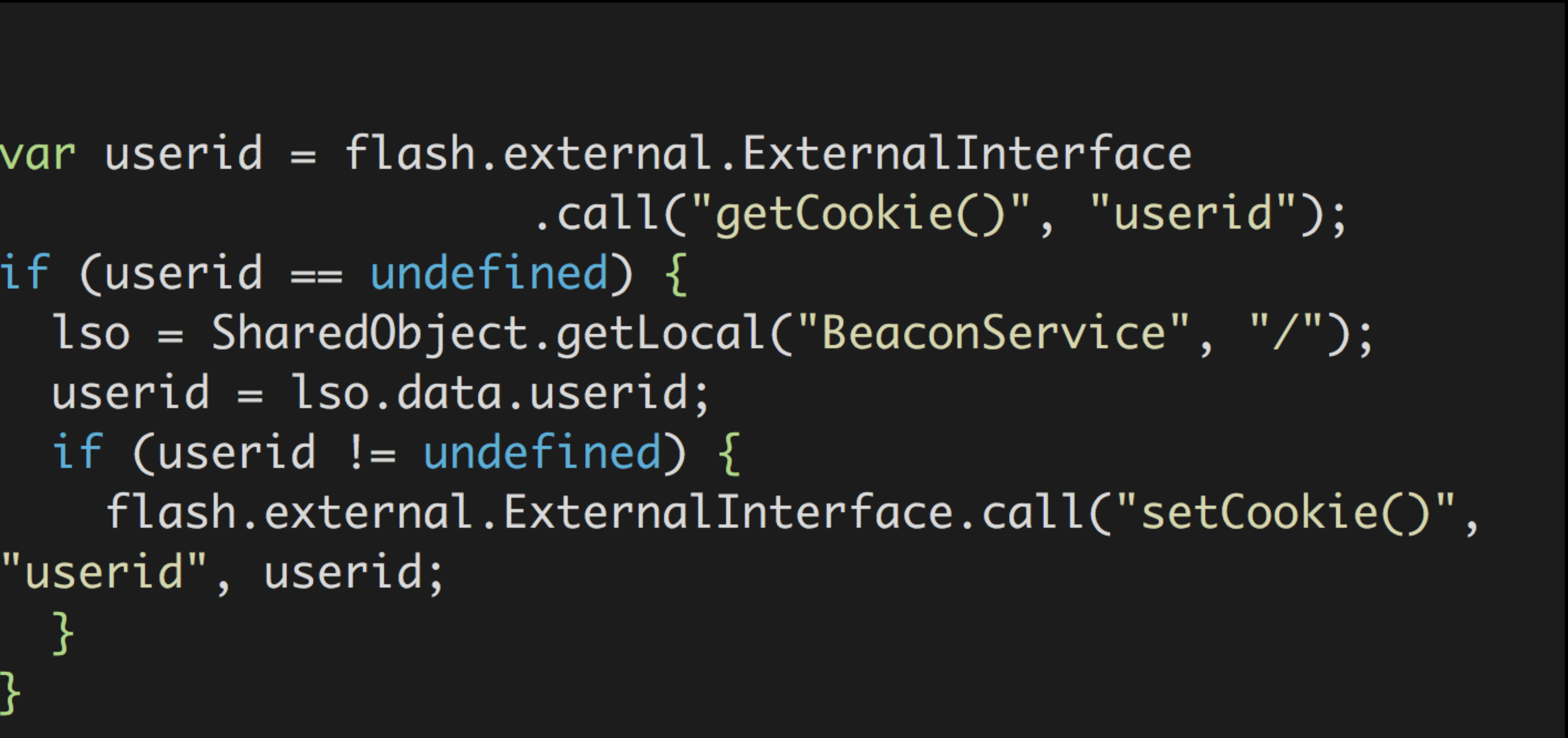
Re-spawning/“Supercookies”



Using Flash

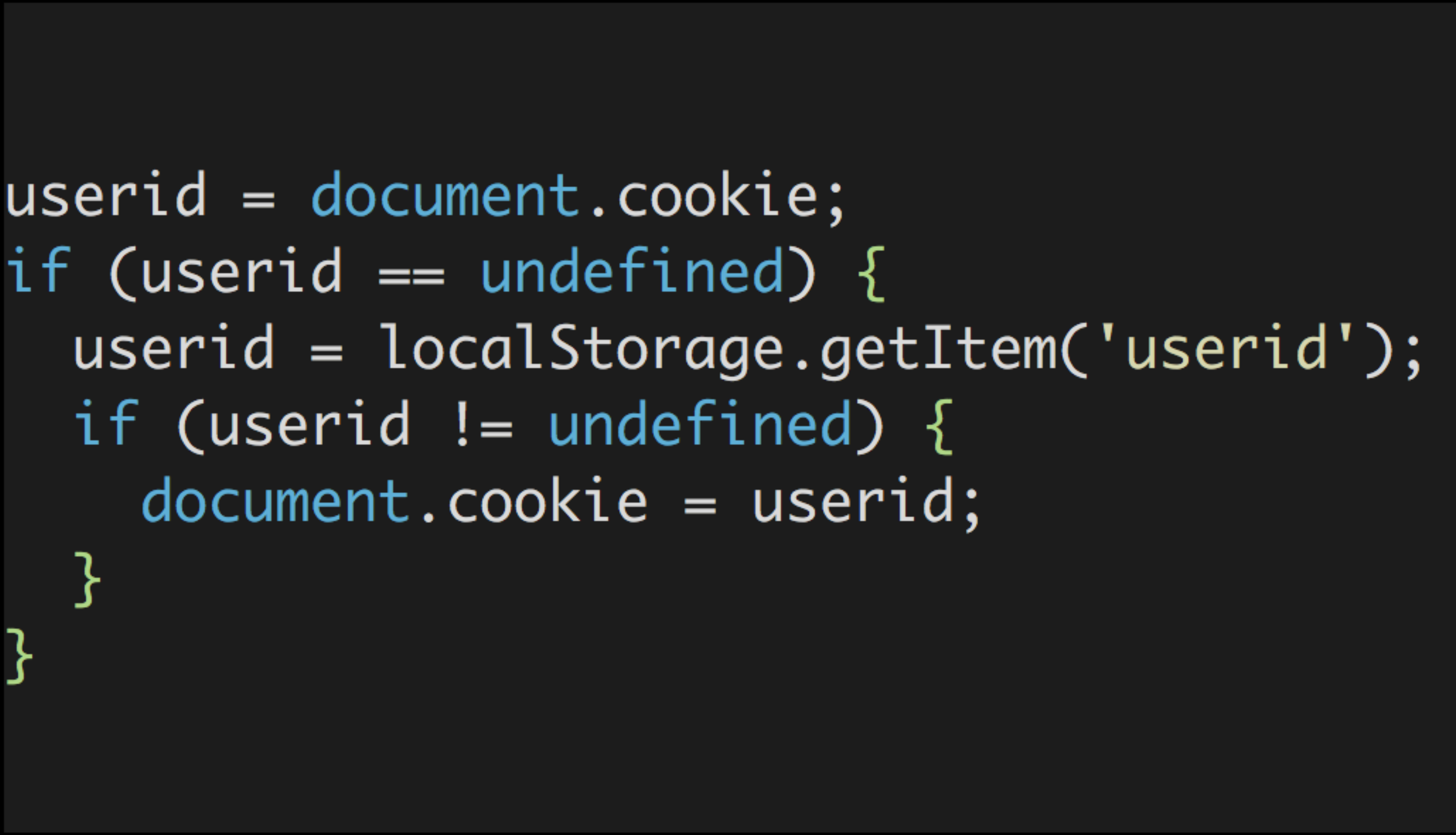


```
document.createElement('div').setAttribute('id', 'swf');

flashvars.everdata = 'userid=123';

swfobject.embedSWF('evercookie.swf', 'swf', .., flashvars);
```



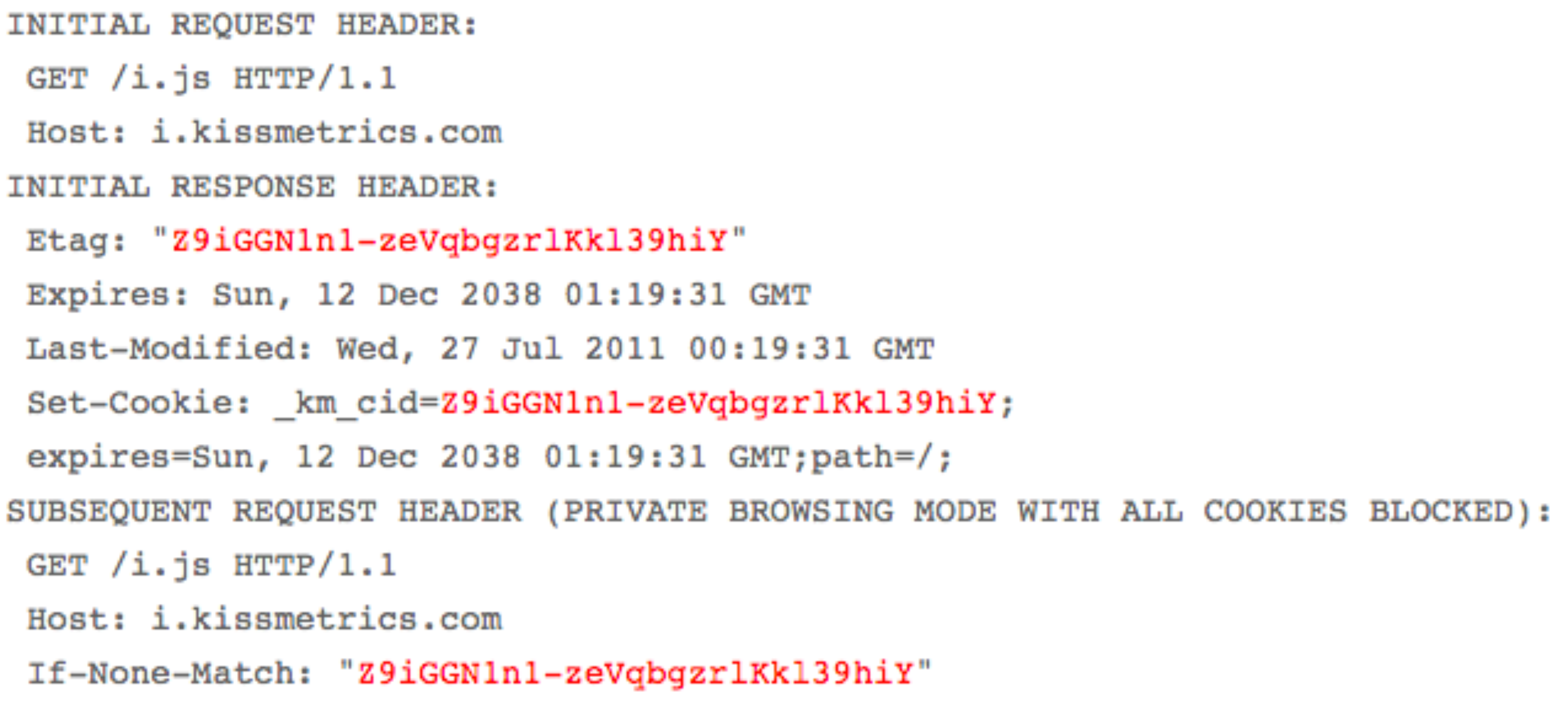
```
var userid = flash.external.ExternalInterface
                    .call("getCookie()", "userid");
if (userid == undefined) {
  lso = SharedObject.getLocal("BeaconService", "/");
  userid = lso.data.userid;
  if (userid != undefined) {
    flash.external.ExternalInterface.call("setCookie()",
"userid", userid;
  }
}
```

HTML localStorage



```
userid = document.cookie;
if (userid == undefined) {
  userid = localStorage.getItem('userid');
  if (userid != undefined) {
    document.cookie = userid;
  }
}
```

ETag

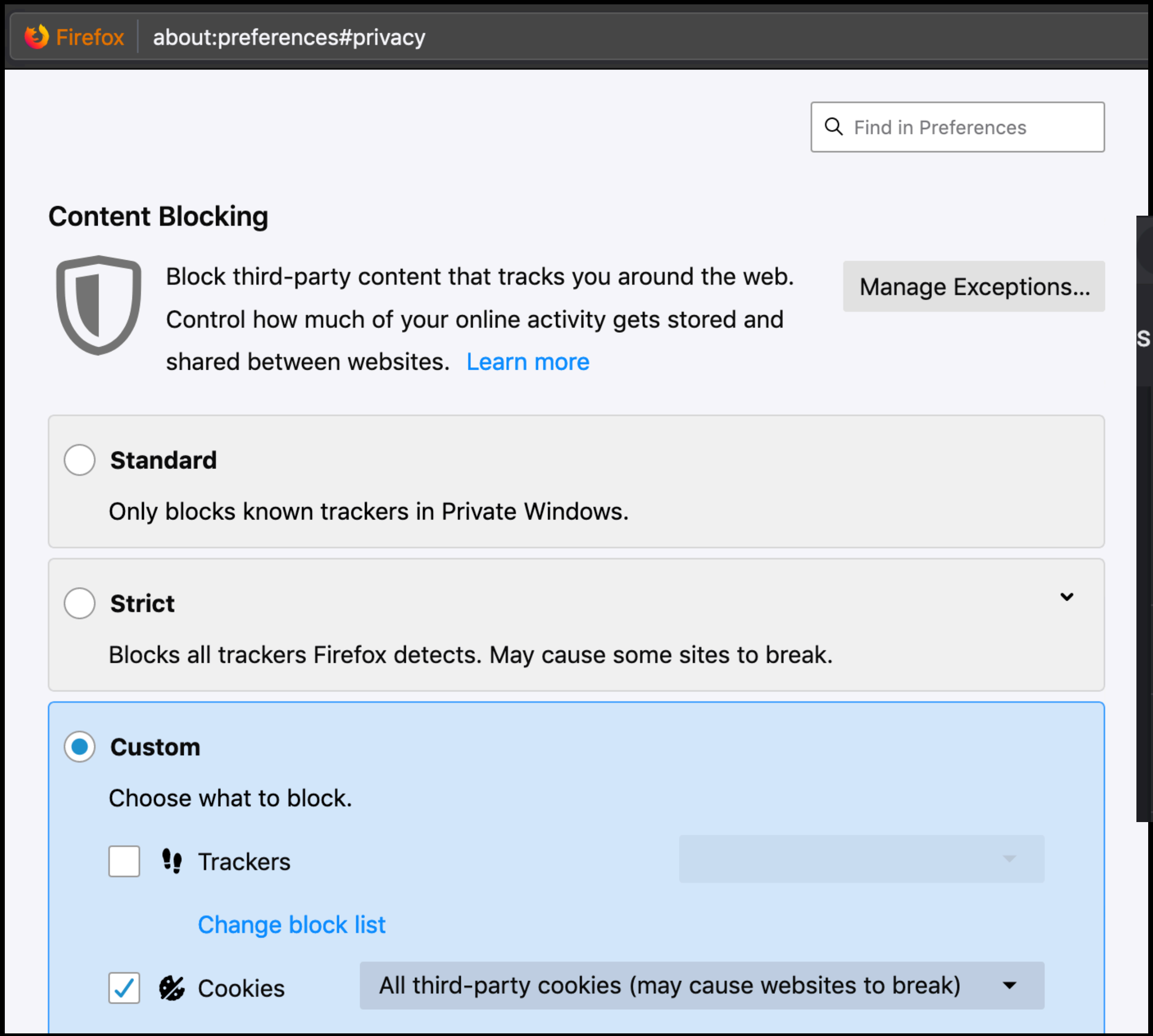


```
INITIAL REQUEST HEADER:
 GET /i.js HTTP/1.1
 Host: i.kissmetrics.com
INITIAL RESPONSE HEADER:
 Etag: "Z9iGGN1n1-zeVqbgzrlKkl39hiY"
 Expires: Sun, 12 Dec 2038 01:19:31 GMT
 Last-Modified: Wed, 27 Jul 2011 00:19:31 GMT
 Set-Cookie: _km_cid=Z9iGGN1n1-zeVqbgzrlKkl39hiY;
 expires=Sun, 12 Dec 2038 01:19:31 GMT;path=/;
SUBSEQUENT REQUEST HEADER (PRIVATE BROWSING MODE WITH ALL COOKIES BLOCKED):
 GET /i.js HTTP/1.1
 Host: i.kissmetrics.com
 If-None-Match: "Z9iGGN1n1-zeVqbgzrlKkl39hiY"
```

Cookie Re-spawning is “Illegal”

Or, at least, companies have been sued for it

Block all 3rd-Party Cookies



Firefox | about:preferences#privacy

Find in Preferences

Content Blocking

Block third-party content that tracks you around the web. Control how much of your online activity gets stored and shared between websites. Learn more

Manage Exceptions...

○ **Standard**

Only blocks known trackers in Private Windows.

○ **Strict**

Blocks all trackers Firefox detects. May cause some sites to break.

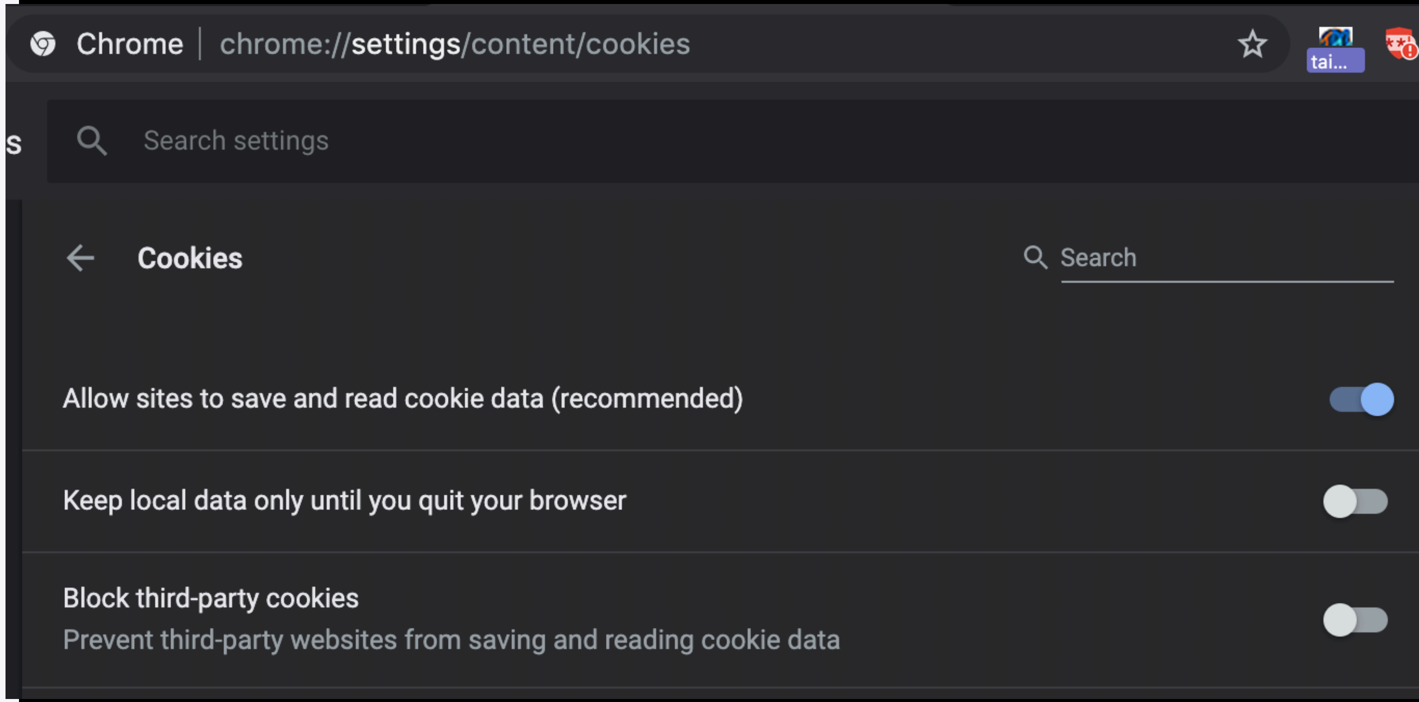
● **Custom**

Choose what to block.

□ Trackers

Change block list

☑ Cookies — All third-party cookies (may cause websites to break)



Chrome | chrome://settings/content/cookies

Search settings

Cookies

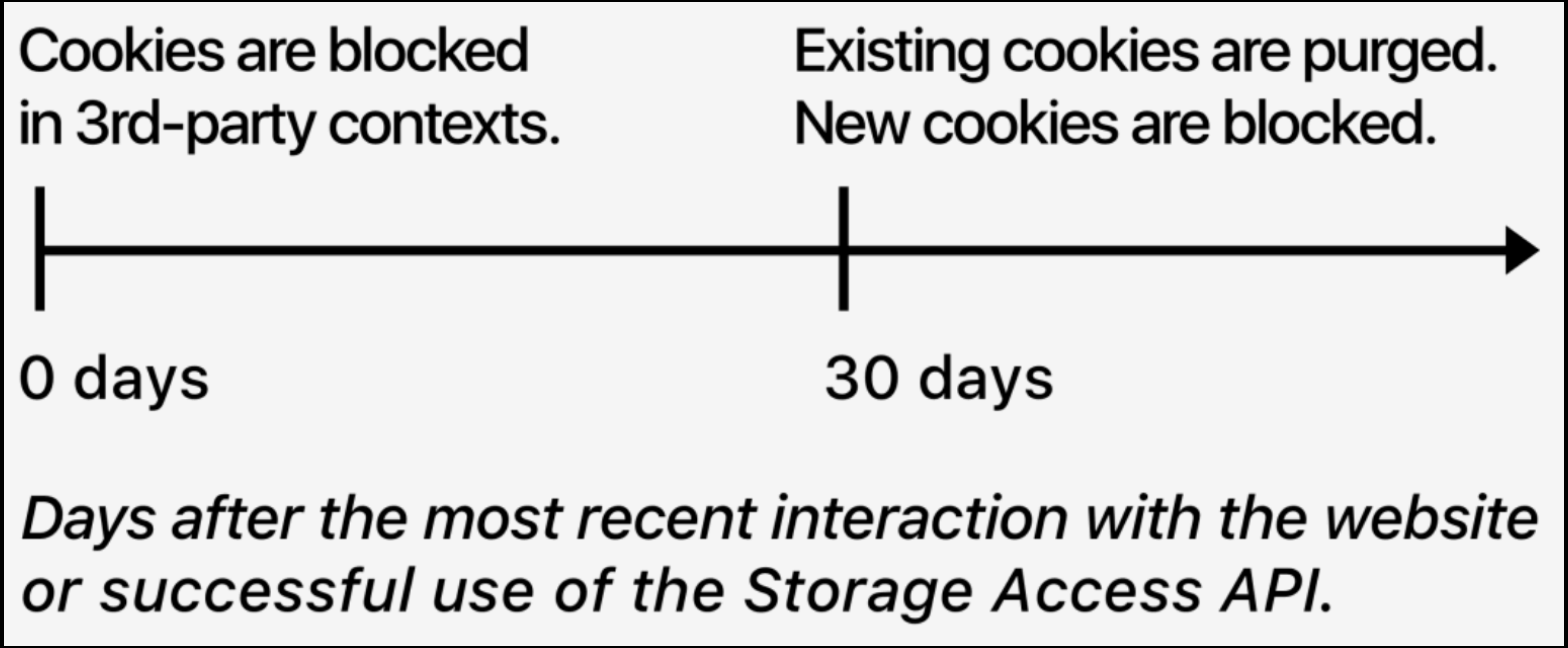
Search

Allow sites to save and read cookie data (recommended)

Keep local data only until you quit your browser

Block third-party cookies
Prevent third-party websites from saving and reading cookie data

Safari ITP 2.1 blocks most 3rd-party Cookies by default



Cookies are blocked in 3rd-party contexts.

Existing cookies are purged. New cookies are blocked.

0 days

30 days

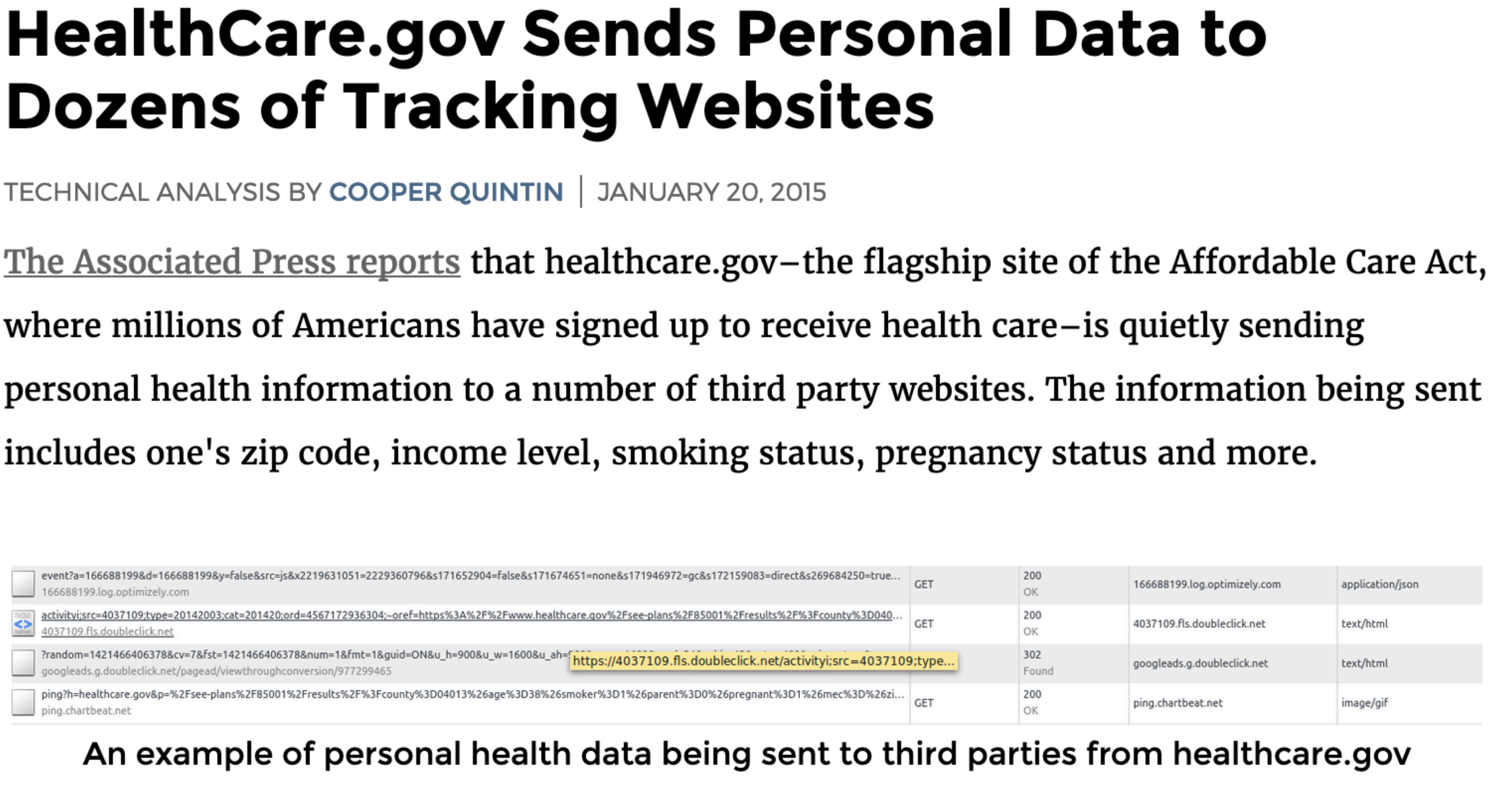
Days after the most recent interaction with the website or successful use of the Storage Access API.

Blocking all 3rd-party cookies is good …

But fingerprinting attacks!

more on this later …

Stripping `Referers`



HealthCare.gov Sends Personal Data to Dozens of Tracking Websites

TECHNICAL ANALYSIS BY COOPER QUINTIN | JANUARY 20, 2015

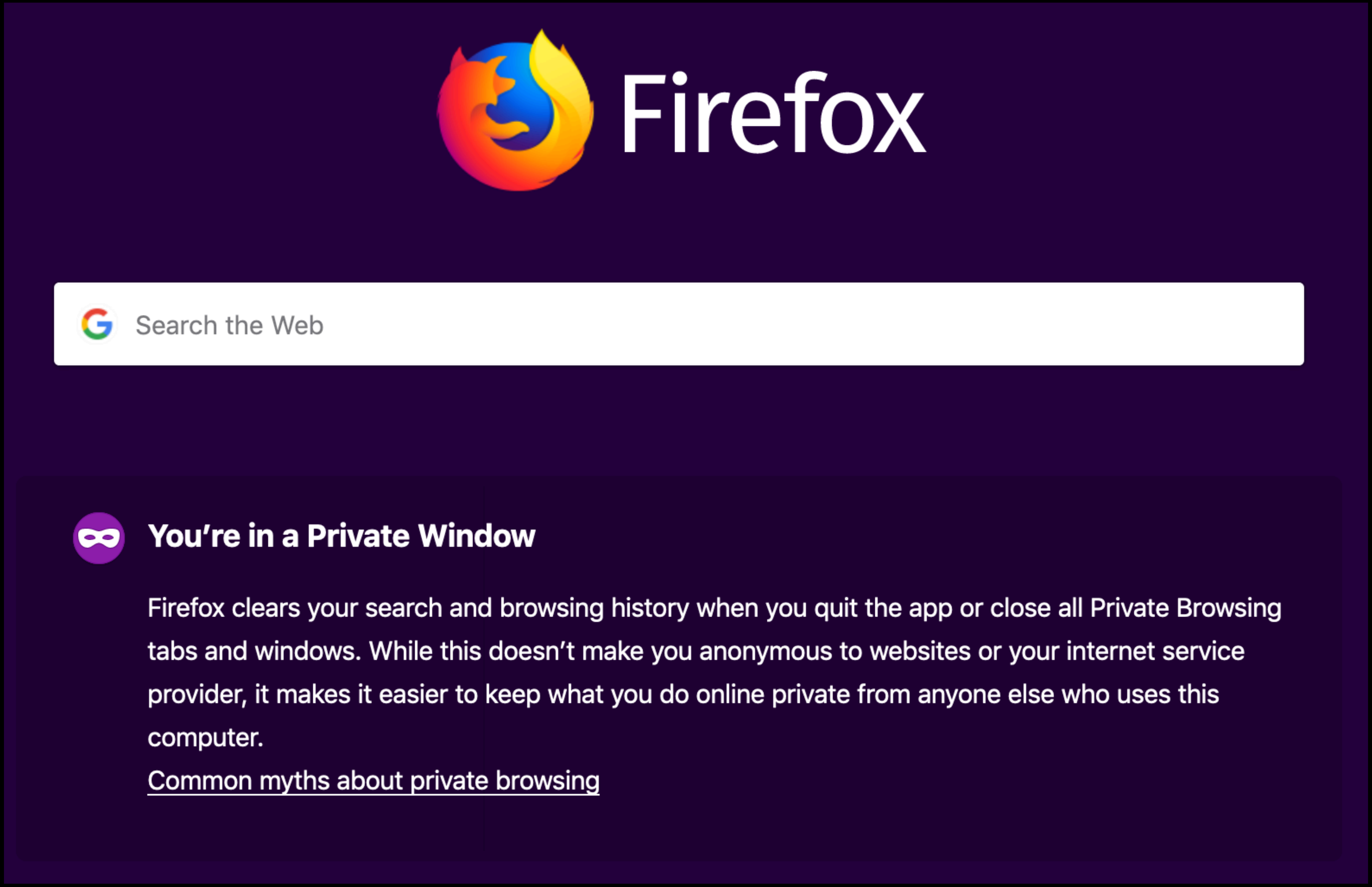
The Associated Press reports that healthcare.gov–the flagship site of the Affordable Care Act, where millions of Americans have signed up to receive health care–is quietly sending personal health information to a number of third party websites. The information being sent includes one's zip code, income level, smoking status, pregnancy status and more.

```
event?a=166688199&d=166688199&y=false&src=js&x2219631051=2229360796&s171652904=false&s171674651=none&s171946972=gc&s172159083=direct&s269684250=true...   GET   200 OK      166688199.log.optimizely.com   application/json
166688199.log.optimizely.com
activityi;src=4037109;type=20142003;cat=201420;ord=4567172936304;~oref=https%3A%2F%2Fwww.healthcare.gov%2Fsee-plans%2F85001%2Fresults%2F%3Fcounty%3D040...   GET   200 OK      4037109.fls.doubleclick.net    text/html
4037109.fls.doubleclick.net
?random=1421466406378&cv=7&fst=1421466406378&num=1&fmt=1&guid=ON&u_h=900&u_w=1600&u_ah=   https://4037109.fls.doubleclick.net/activityi;src=4037109;type...   302 Found   googleads.g.doubleclick.net    text/html
googleads.g.doubleclick.net/pagead/viewthroughconversion/977299465
ping?h=healthcare.gov&p=%2Fsee-plans%2F85001%2Fresults%2F%3Fcounty%3D04013%26age%3D38%26smoker%3D1%26parent%3D0%26pregnant%3D1%26mec%3D%26zi...   GET   200 OK      ping.chartbeat.net             image/gif
ping.chartbeat.net
```

An example of personal health data being sent to third parties from healthcare.gov

https://www.eff.org/deeplinks/2015/01/healthcare.gov-sends-personal-data

Firefox Private Browsing strips paths from `Referer` by default



You're in a Private Window

Firefox clears your search and browsing history when you quit the app or close all Private Browsing tabs and windows. While this doesn't make you anonymous to websites or your internet service provider, it makes it easier to keep what you do online private from anyone else who uses this computer.

Common myths about private browsing

Firefox

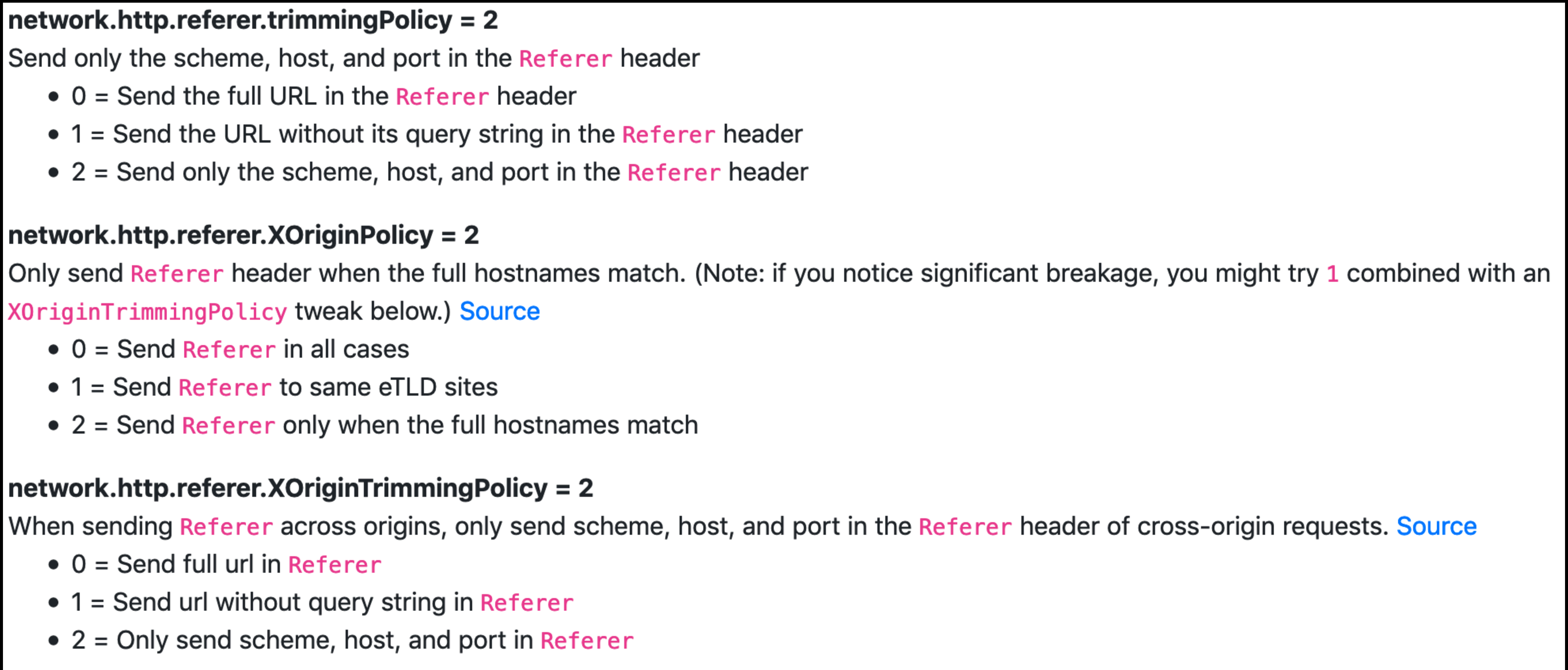
```
Referer:
https://www.reddit.com/
r/privacy/comments/
Preventing_data_leaks_by
_stripping_path_informat
ion_in_HTTP_Referrers/
```

```
Referer:
https://www.reddit.com/
```

```
Referer: https://
www.healthcare.gov/see-
plans/85601/results/?
county=04019&age=40&smok
er=1&pregnant=1&zip=8560
1&state=AZ&income=35000
```

```
Referer:
https://www.healthcare.gov/
```

More `Referer` Protections in Firefox



network.http.referer.trimmingPolicy = 2

Send only the scheme, host, and port in the `Referer` header

- 0 = Send the full URL in the `Referer` header
- 1 = Send the URL without its query string in the `Referer` header
- 2 = Send only the scheme, host, and port in the `Referer` header

network.http.referer.XOriginPolicy = 2

Only send `Referer` header when the full hostnames match. (Note: if you notice significant breakage, you might try `1` combined with an `XOriginTrimmingPolicy` tweak below.) Source

- 0 = Send `Referer` in all cases
- 1 = Send `Referer` to same eTLD sites
- 2 = Send `Referer` only when the full hostnames match

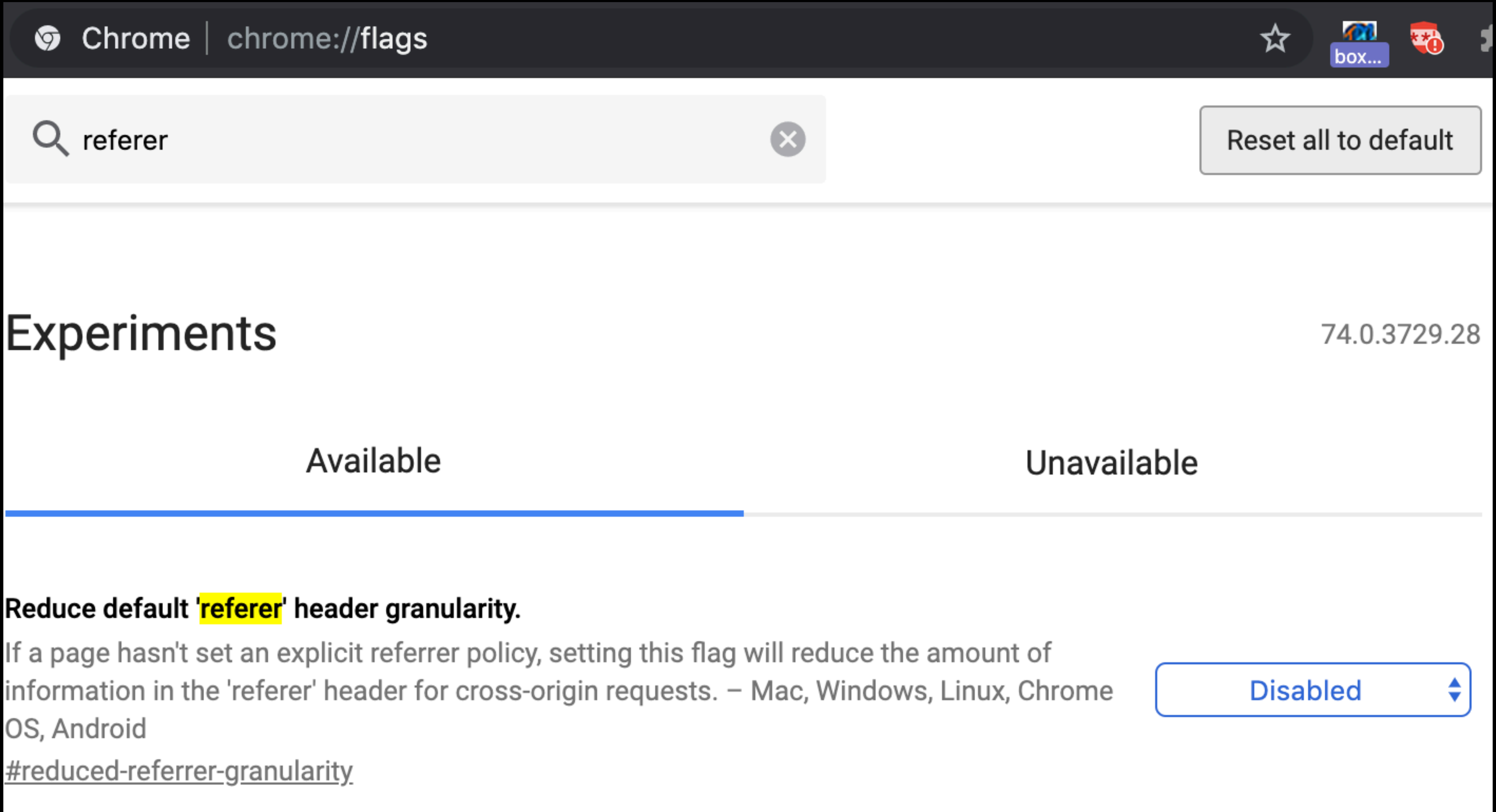
network.http.referer.XOriginTrimmingPolicy = 2

When sending `Referer` across origins, only send scheme, host, and port in the `Referer` header of cross-origin requests. Source

- 0 = Send full url in `Referer`
- 1 = Send url without query string in `Referer`
- 2 = Only send scheme, host, and port in `Referer`

https://www.privacytools.io/#about_config

#reduced-referrer-granularity in chrome://flags



referer

Reset all to default

Experiments

74.0.3729.28

Available Unavailable

Reduce default 'referer' header granularity.

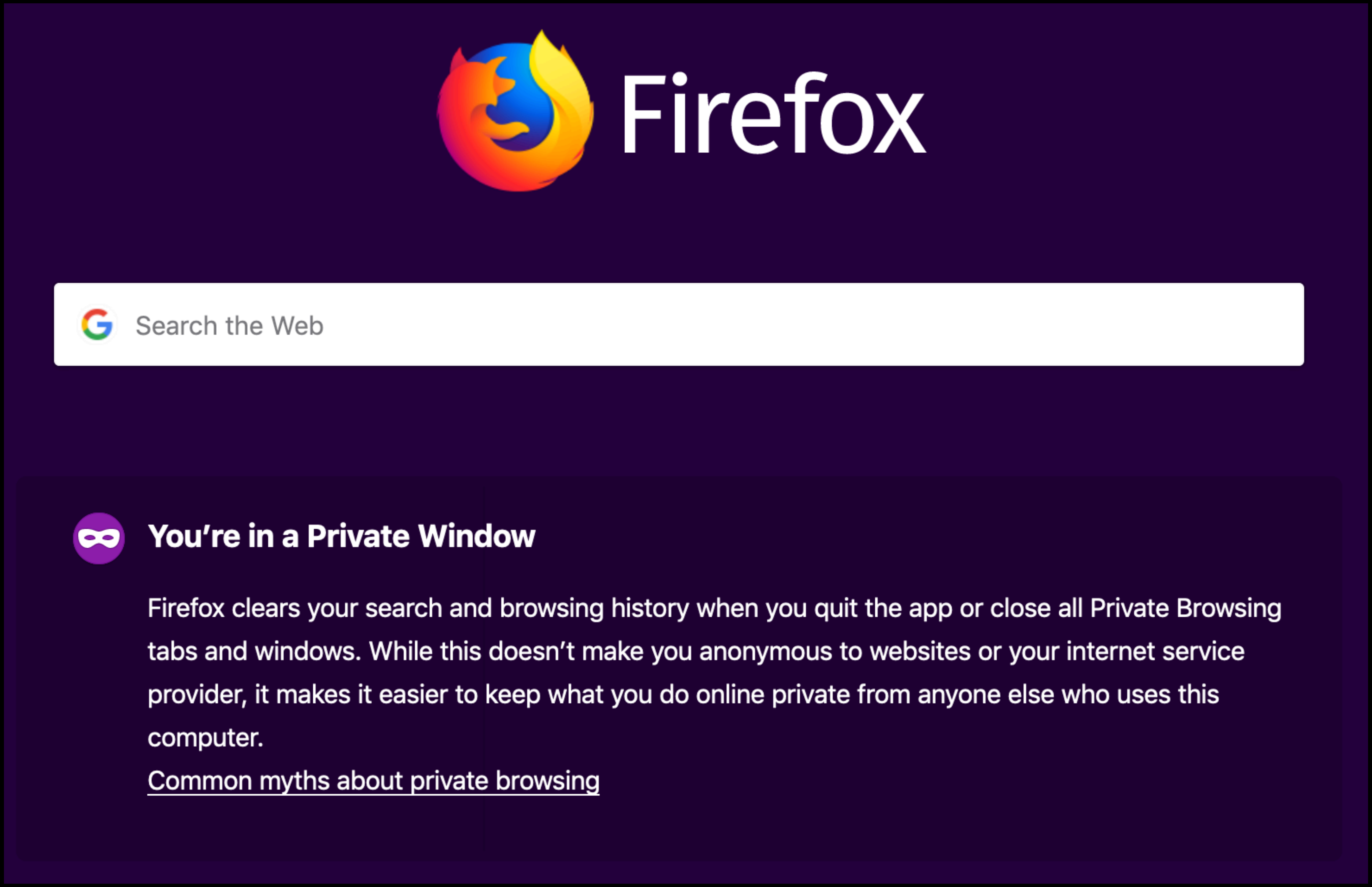
If a page hasn't set an explicit referrer policy, setting this flag will reduce the amount of information in the 'referer' header for cross-origin requests. – Mac, Windows, Linux, Chrome OS, Android

#reduced-referrer-granularity

Disabled

Tracking Protection blocks data to trackers

Firefox Private Browsing includes Tracking Protection by default

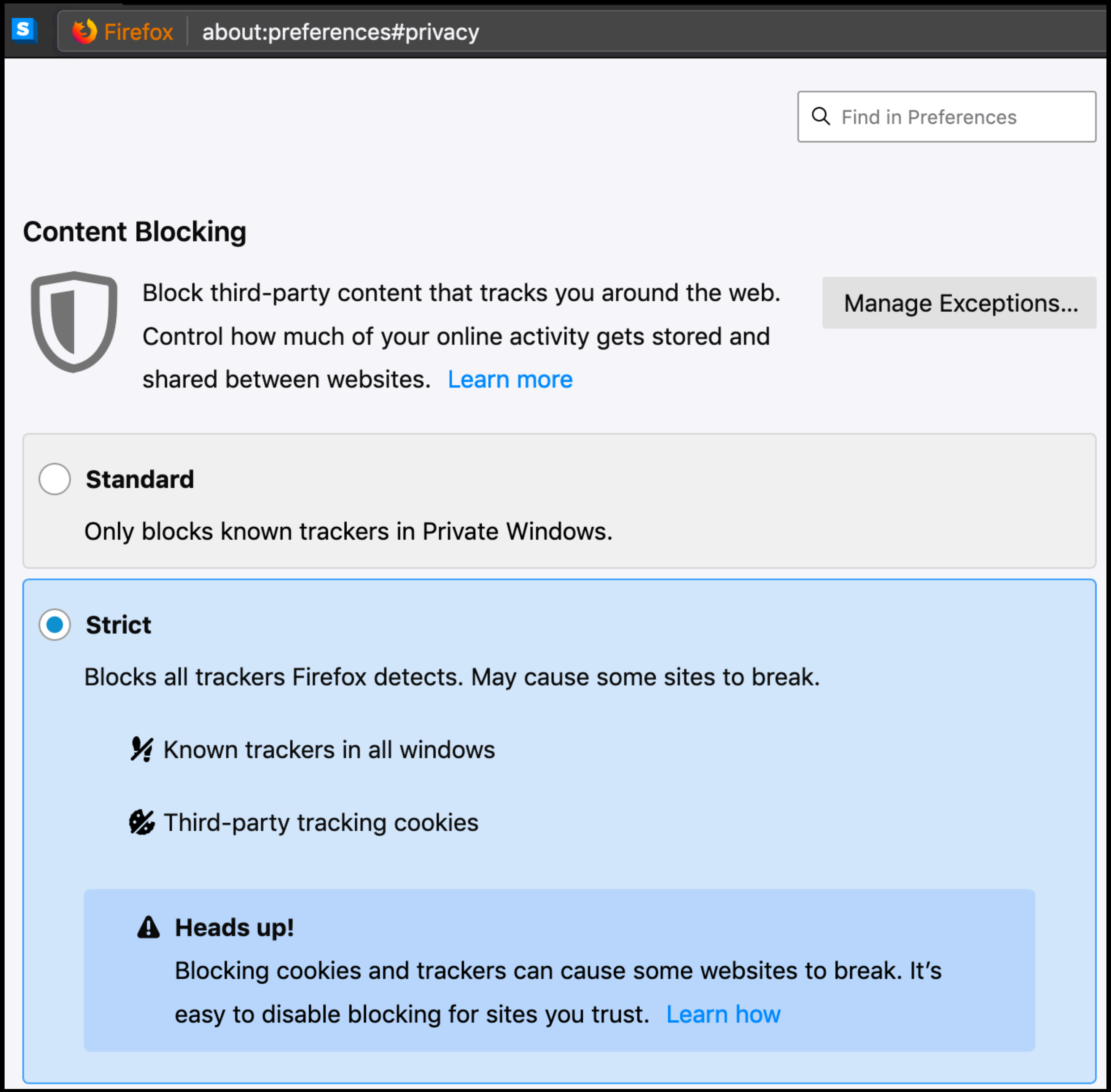


You’re in a Private Window

Firefox clears your search and browsing history when you quit the app or close all Private Browsing tabs and windows. While this doesn’t make you anonymous to websites or your internet service provider, it makes it easier to keep what you do online private from anyone else who uses this computer.

Common myths about private browsing

You can enable Tracking Protection for all of Firefox



Content Blocking

Block third-party content that tracks you around the web. Control how much of your online activity gets stored and shared between websites. Learn more

○ **Standard**

Only blocks known trackers in Private Windows.

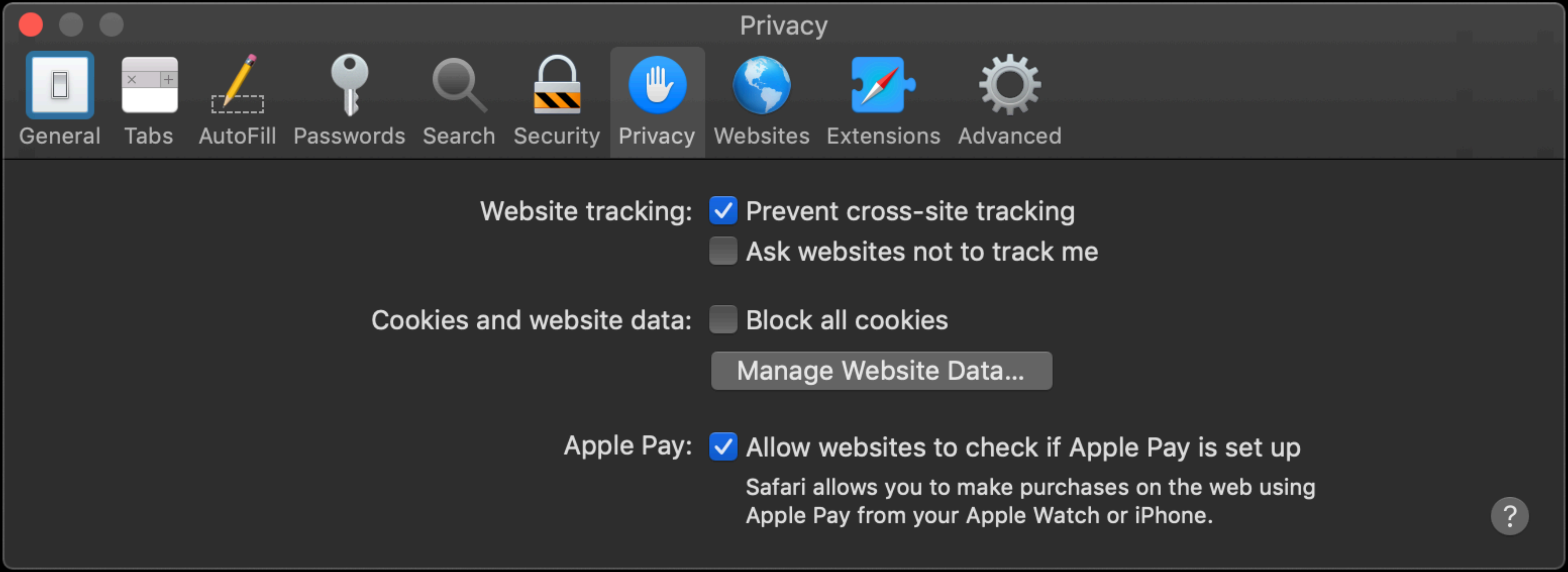
● **Strict**

Blocks all trackers Firefox detects. May cause some sites to break.

- Known trackers in all windows
- Third-party tracking cookies

Heads up!
Blocking cookies and trackers can cause some websites to break. It’s easy to disable blocking for sites you trust. Learn how

Safari includes Tracking Protection by default



Website tracking: ☑ Prevent cross-site tracking

□ Ask websites not to track me

Cookies and website data: □ Block all cookies

Manage Website Data...

Apple Pay: ☑ Allow websites to check if Apple Pay is set up

Safari allows you to make purchases on the web using Apple Pay from your Apple Watch or iPhone.

?

Tracking Protection Add-ons and Extensions

PRIVACY BADGER

uBlock Origin

GHOSTERY®

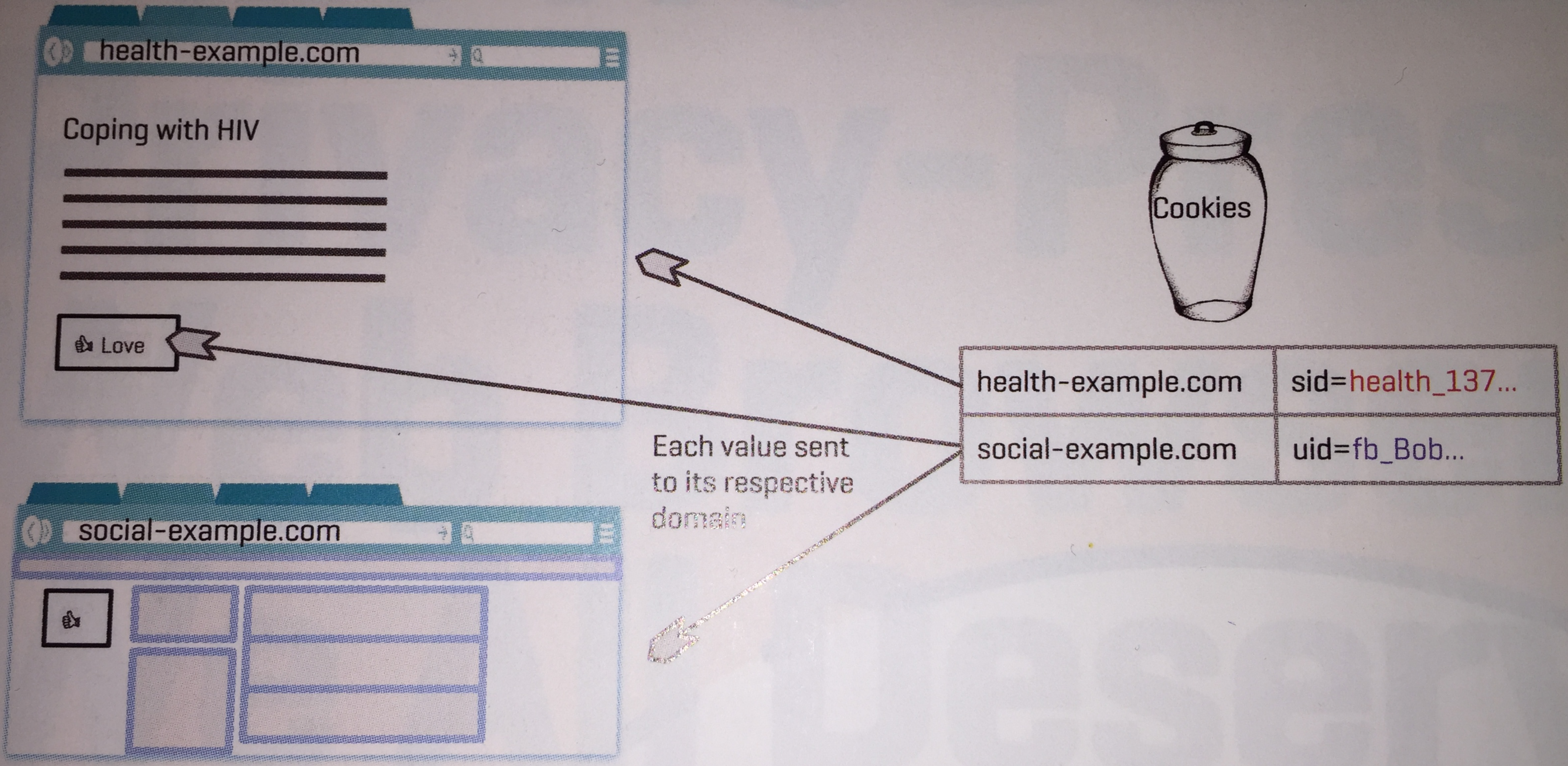
Tracking Protection is good …

… but what if trackers evade the block-lists?

First-Party Isolation

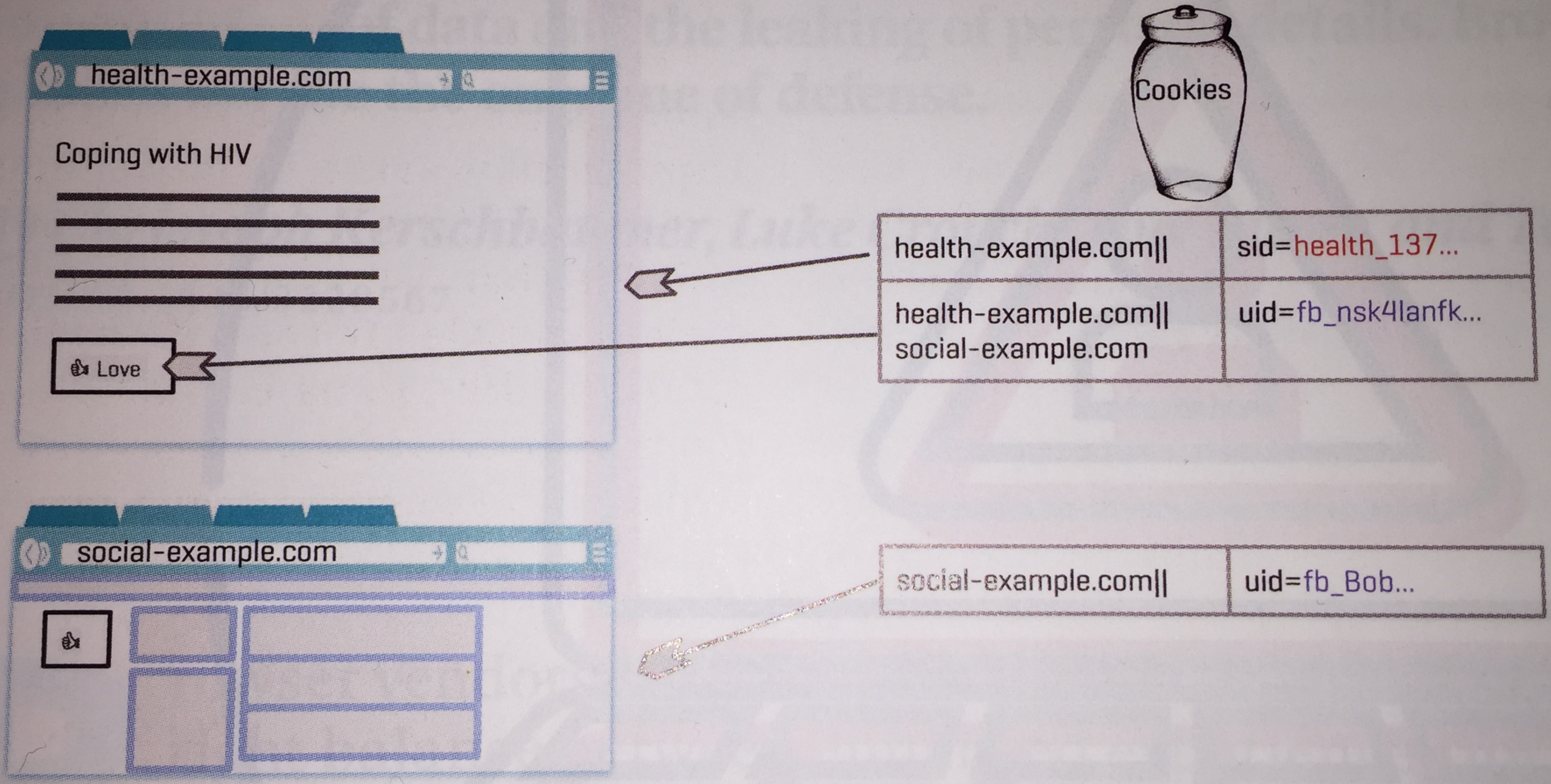
Only in Firefox and Tor

Figure 1. Without first party isolation, the same cookie is sent no matter the first party domain.



health-example.com	sid=health_137...
social-example.com	uid=fb_Bob...

Figure 2. With first party isolation, separate cookies are sent depending on the first party domain.



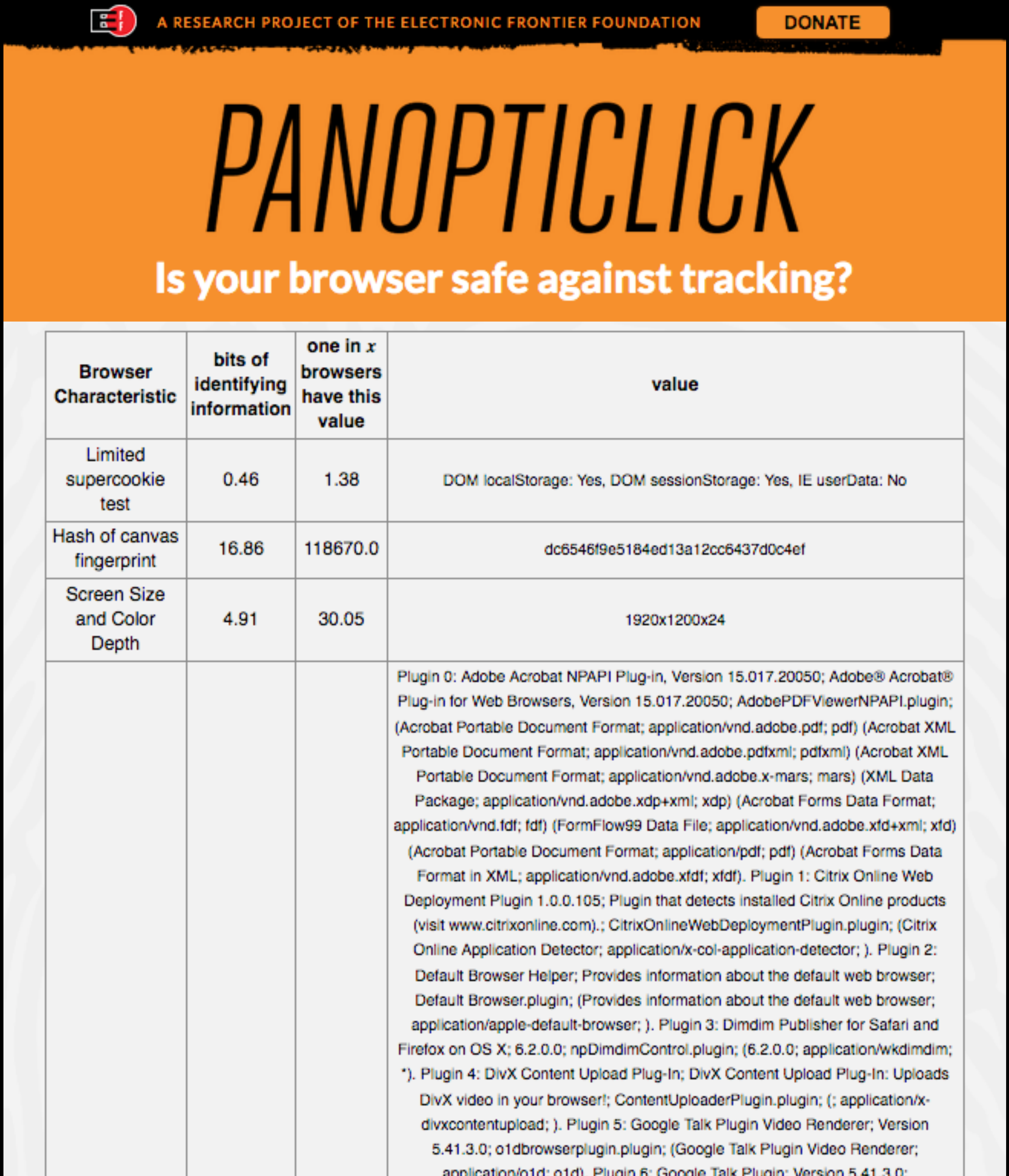
health-example.com||	sid=health_137...
health-example.com|| social-example.com	uid=fb_nsk4lanfk...

social-example.com||	uid=fb_Bob...

Isolating all 3rd-party cookies is good …

But fingerprinting attacks!

more on this NOW!



A RESEARCH PROJECT OF THE ELECTRONIC FRONTIER FOUNDATION

DONATE

PANOPTICLICK

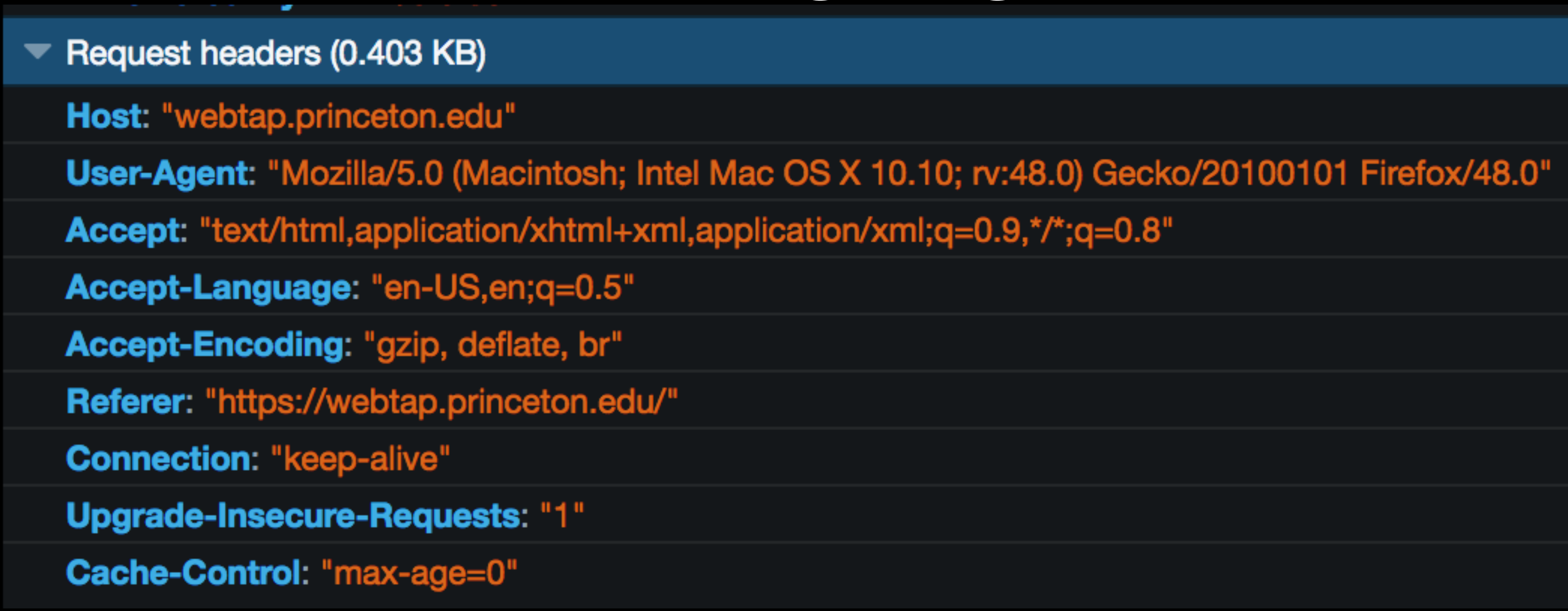
Is your browser safe against tracking?

Browser Characteristic	bits of identifying information	one in *x* browsers have this value	value
Limited supercookie test	0.46	1.38	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No
Hash of canvas fingerprint	16.86	118670.0	dc6546f9e5184ed13a12cc6437d0c4ef
Screen Size and Color Depth	4.91	30.05	1920x1200x24
			Plugin 0: Adobe Acrobat NPAPI Plug-in, Version 15.017.20050; Adobe® Acrobat® Plug-in for Web Browsers, Version 15.017.20050; AdobePDFViewerNPAPI.plugin; (Acrobat Portable Document Format; application/vnd.adobe.pdf; pdf) (Acrobat XML Portable Document Format; application/vnd.adobe.pdfxml; pdfxml) (Acrobat XML Portable Document Format; application/vnd.adobe.x-mars; mars) (XML Data Package; application/vnd.adobe.xdp+xml; xdp) (Acrobat Forms Data Format; application/vnd.fdf; fdf) (FormFlow99 Data File; application/vnd.adobe.xfd+xml; xfd) (Acrobat Portable Document Format; application/pdf; pdf) (Acrobat Forms Data Format in XML; application/vnd.adobe.xfdf; xfdf). Plugin 1: Citrix Online Web Deployment Plugin 1.0.0.105; Plugin that detects installed Citrix Online products (visit www.citrixonline.com).; CitrixOnlineWebDeploymentPlugin.plugin; (Citrix Online Application Detector; application/x-col-application-detector;). Plugin 2: Default Browser Helper; Provides information about the default web browser; Default Browser.plugin; (Provides information about the default web browser; application/apple-default-browser;). Plugin 3: Dimdim Publisher for Safari and Firefox on OS X; 6.2.0.0; npDimdimControl.plugin; (6.2.0.0; application/wkdimdim; *). Plugin 4: DivX Content Upload Plug-In; DivX Content Upload Plug-In: Uploads DivX video in your browser!; ContentUploaderPlugin.plugin; (; application/x-divxcontentupload;). Plugin 5: Google Talk Plugin Video Renderer; Version 5.41.3.0; o1dbrowserplugin.plugin; (Google Talk Plugin Video Renderer; application/o1d; o1d). Plugin 6: Google Talk Plugin; Version 5.41.3.0;

Passive Fingerprints

Don’t require code execution

User-Agent, IP, Accept-Language, etc.

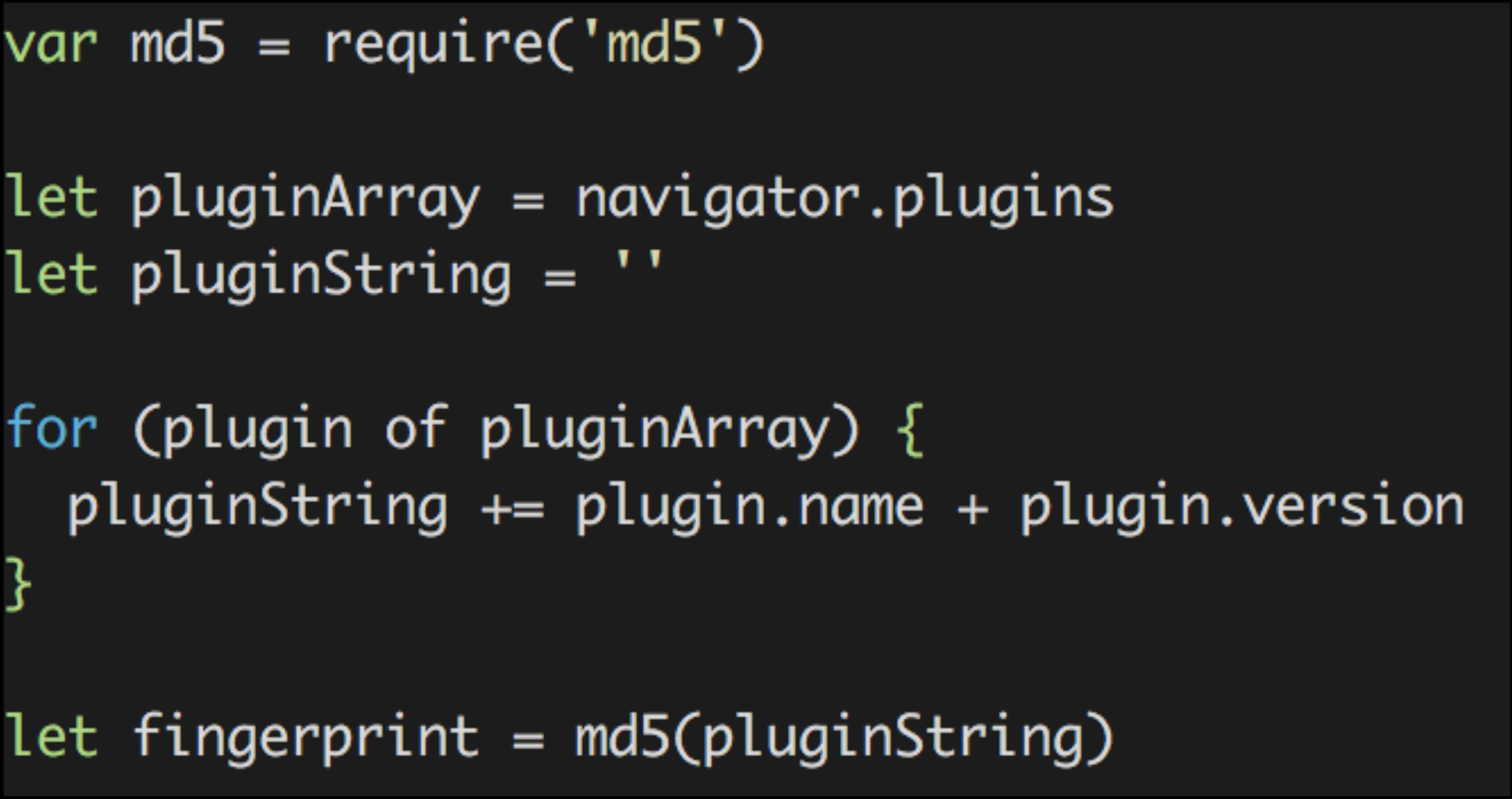


```
Request headers (0.403 KB)
Host: "webtap.princeton.edu"
User-Agent: "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:48.0) Gecko/20100101 Firefox/48.0"
Accept: "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8"
Accept-Language: "en-US,en;q=0.5"
Accept-Encoding: "gzip, deflate, br"
Referer: "https://webtap.princeton.edu/"
Connection: "keep-alive"
Upgrade-Insecure-Requests: "1"
Cache-Control: "max-age=0"
```

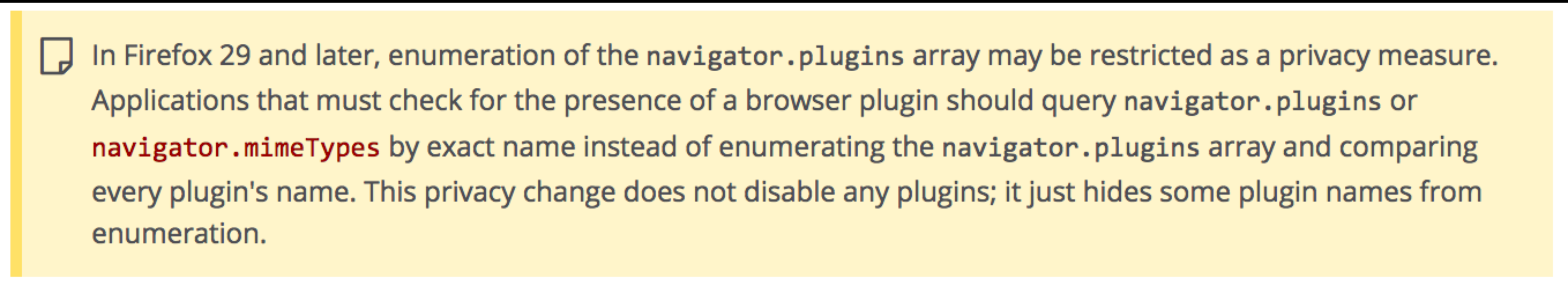
Active Fingerprints

JavaScript code executes on your device

Plugin Enumeration



```
var md5 = require('md5')

let pluginArray = navigator.plugins
let pluginString = ''

for (plugin of pluginArray) {
  pluginString += plugin.name + plugin.version
}

let fingerprint = md5(pluginString)
```

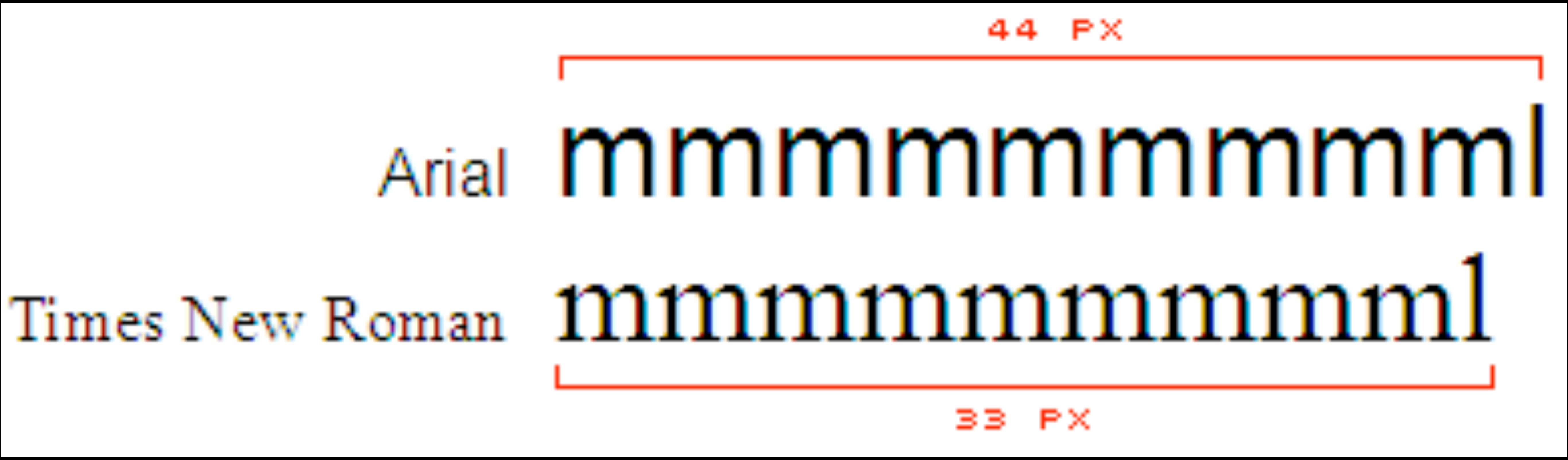


In Firefox 29 and later, enumeration of the `navigator.plugins` array may be restricted as a privacy measure. Applications that must check for the presence of a browser plugin should query `navigator.plugins` or `navigator.mimeTypes` by exact name instead of enumerating the `navigator.plugins` array and comparing every plugin's name. This privacy change does not disable any plugins; it just hides some plugin names from enumeration.

Okay but …

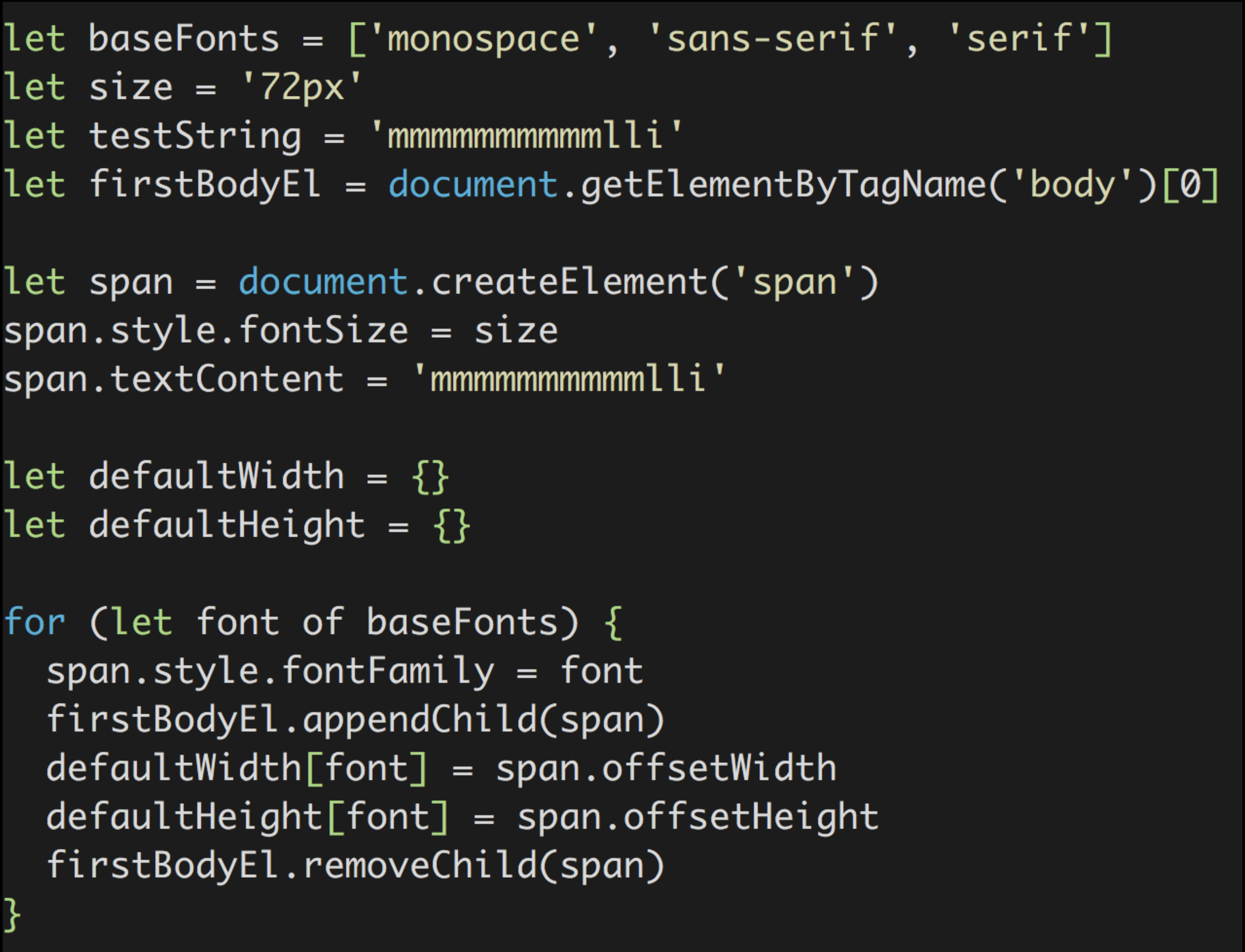
… enumeration is still possible via sniffing, like …

Font Enumeration



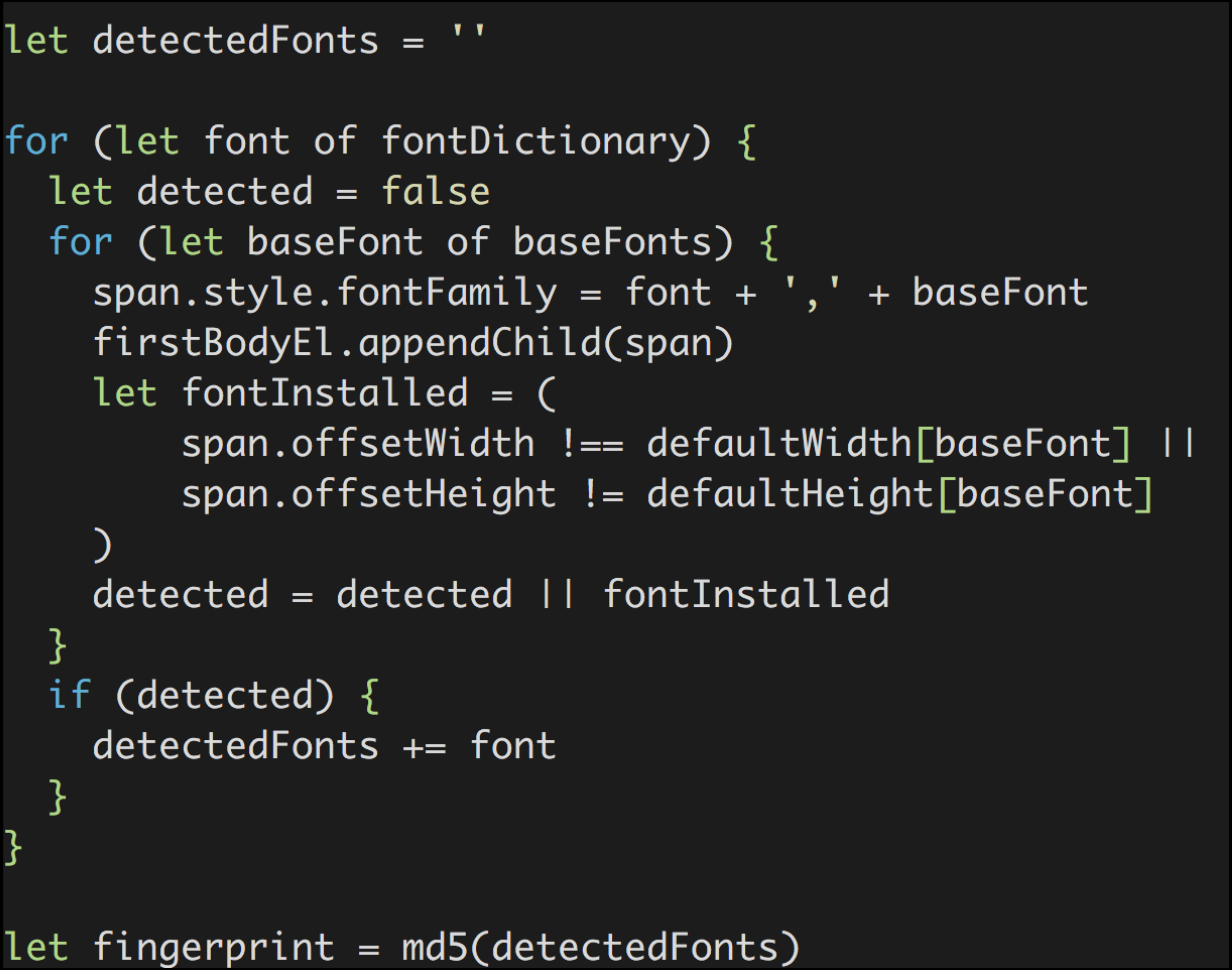
http://www.lalit.org/lab/javascript-css-font-detect/

Measure default fonts



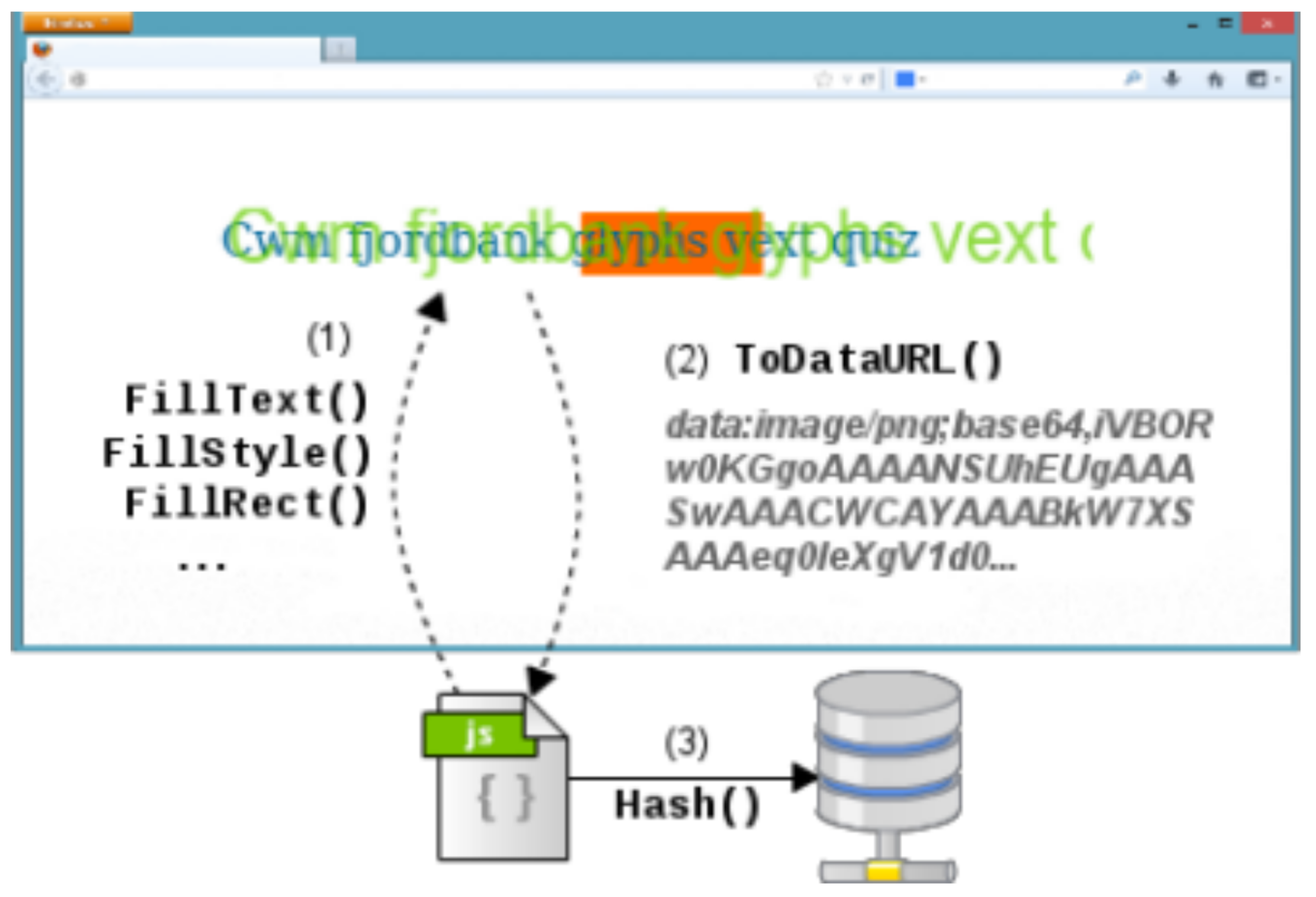
```
let baseFonts = ['monospace', 'sans-serif', 'serif']
let size = '72px'
let testString = 'mmmmmmmmmmlli'
let firstBodyEl = document.getElementByTagName('body')[0]

let span = document.createElement('span')
span.style.fontSize = size
span.textContent = 'mmmmmmmmmmlli'

let defaultWidth = {}
let defaultHeight = {}

for (let font of baseFonts) {
  span.style.fontFamily = font
  firstBodyEl.appendChild(span)
  defaultWidth[font] = span.offsetWidth
  defaultHeight[font] = span.offsetHeight
  firstBodyEl.removeChild(span)
}
```

Measure dictionary of fonts

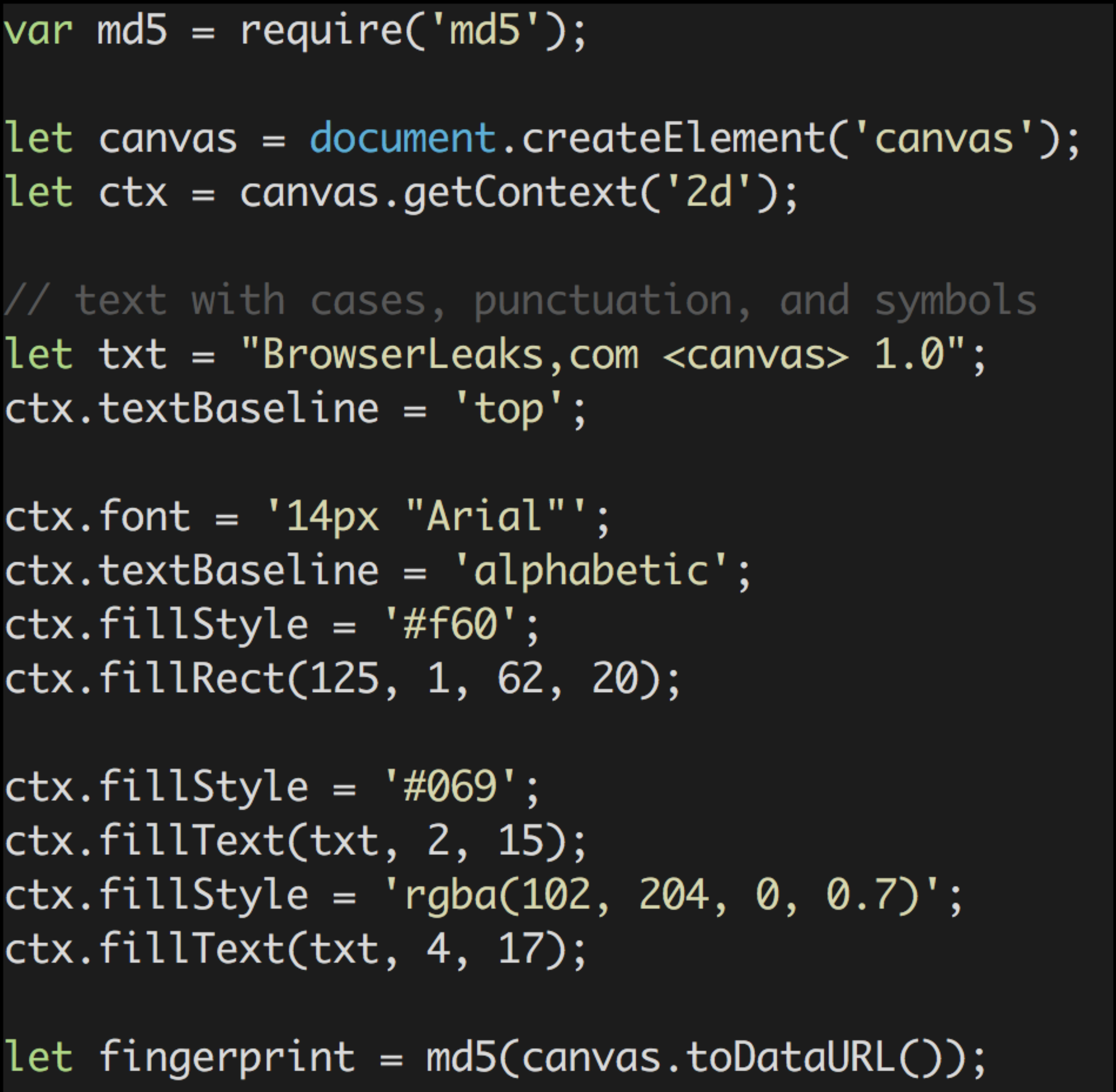


```
let detectedFonts = ''

for (let font of fontDictionary) {
  let detected = false
  for (let baseFont of baseFonts) {
    span.style.fontFamily = font + ',' + baseFont
    firstBodyEl.appendChild(span)
    let fontInstalled = (
        span.offsetWidth !== defaultWidth[baseFont] ||
        span.offsetHeight != defaultHeight[baseFont]
    )
    detected = detected || fontInstalled
  }
  if (detected) {
    detectedFonts += font
  }
}

let fingerprint = md5(detectedFonts)
```

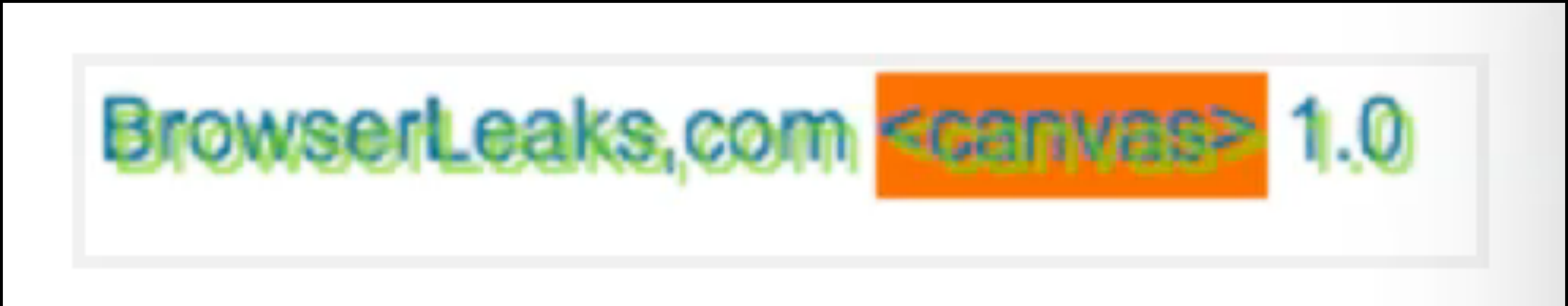
Canvas Fingerprint



data:image/png;base64,iVBOR
w0KGgoAAAANSUhEUgAAA
SwAAACWCAYAAABkW7XS
AAAeq0leXgV1d0...

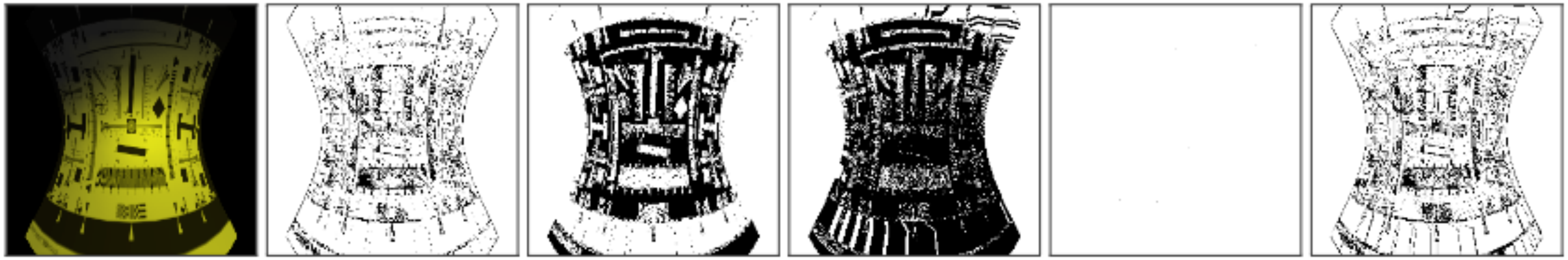


```
var md5 = require('md5');

let canvas = document.createElement('canvas');
let ctx = canvas.getContext('2d');

// text with cases, punctuation, and symbols
let txt = "BrowserLeaks,com <canvas> 1.0";
ctx.textBaseline = 'top';

ctx.font = '14px "Arial"';
ctx.textBaseline = 'alphabetic';
ctx.fillStyle = '#f60';
ctx.fillRect(125, 1, 62, 20);

ctx.fillStyle = '#069';
ctx.fillText(txt, 2, 15);
ctx.fillStyle = 'rgba(102, 204, 0, 0.7)';
ctx.fillText(txt, 4, 17);

let fingerprint = md5(canvas.toDataURL());
```



BrowserLeaks,com <canvas> 1.0

WebGL Fingerprinting



(a) Original (Intel G41)

(b) Group 1 (Radeon HD 2400)

(c) Group 20 (Intel 82945G)

(d) Group 23 (Intel G33/G31)

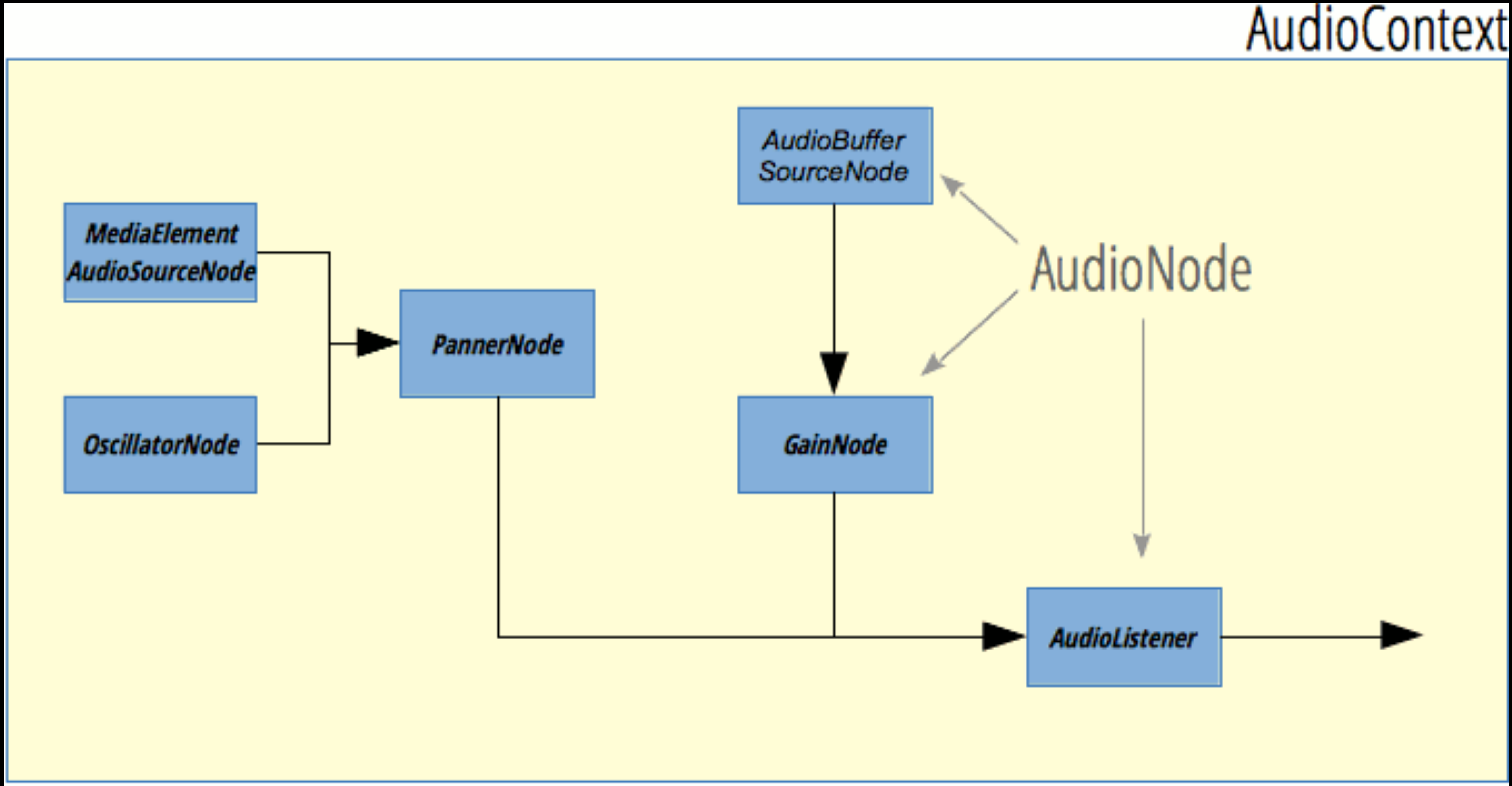
(e) Group 25 (Intel HD Graphics)

(f) Group 36 (GeForce 6200)

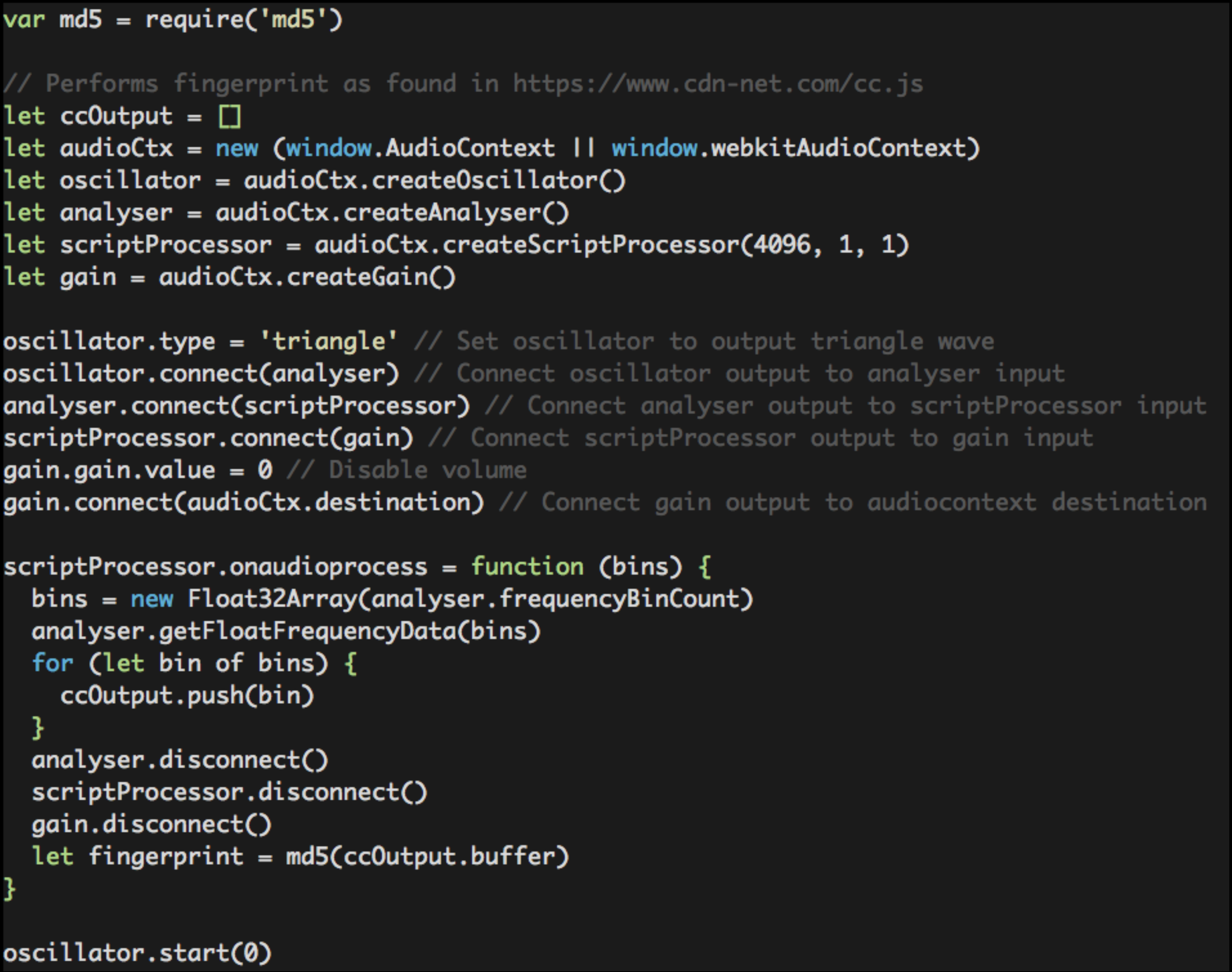
Figure 10: Original render and difference maps for Group 24

http://cseweb.ucsd.edu/~hovav/dist/canvas.pdf

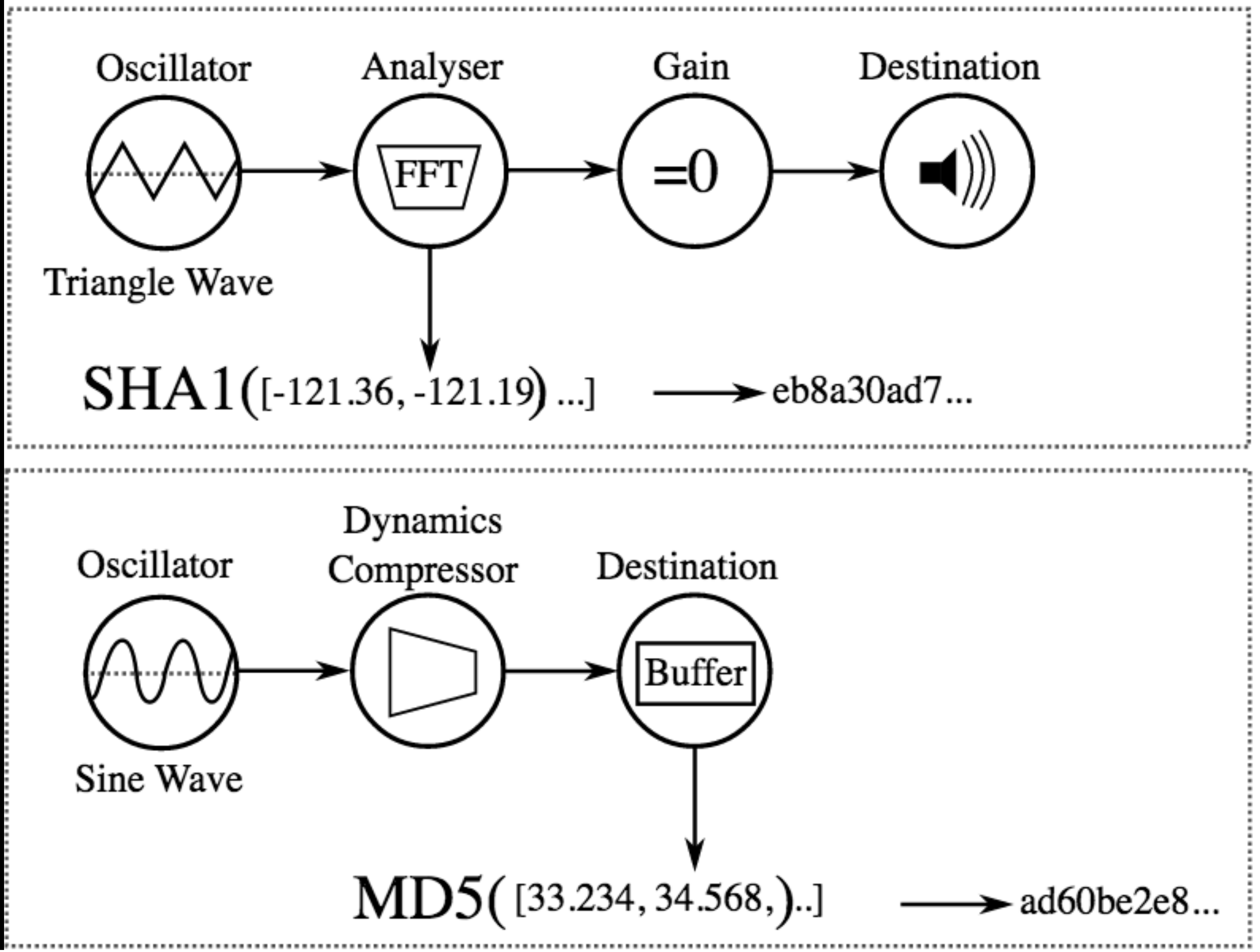
AudioContext

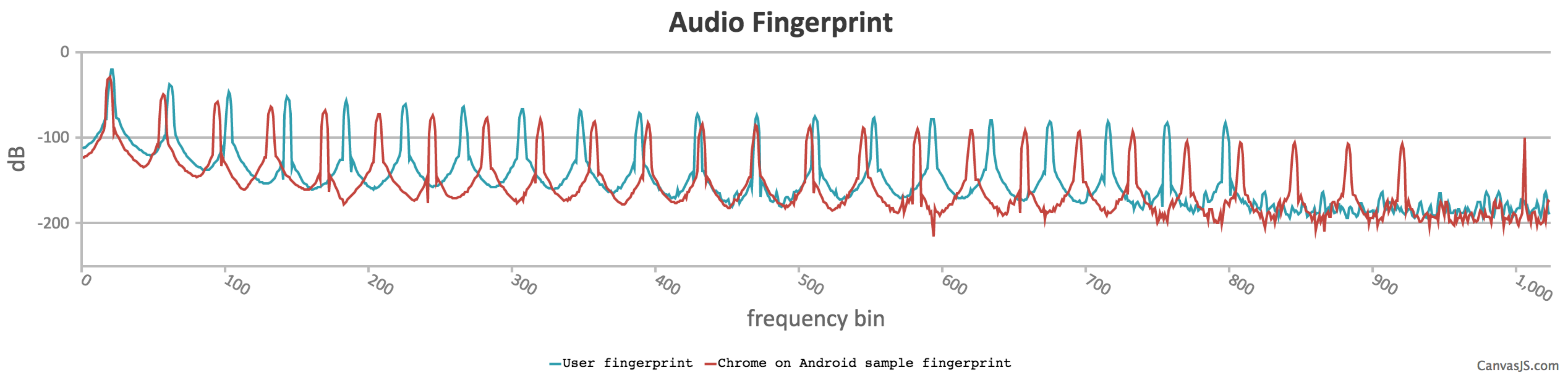


The connected AudioNodes in a given AudioContext create an audio routing graph.



```
var md5 = require('md5')

// Performs fingerprint as found in https://www.cdn-net.com/cc.js
let ccOutput = []
let audioCtx = new (window.AudioContext || window.webkitAudioContext)
let oscillator = audioCtx.createOscillator()
let analyser = audioCtx.createAnalyser()
let scriptProcessor = audioCtx.createScriptProcessor(4096, 1, 1)
let gain = audioCtx.createGain()

oscillator.type = 'triangle' // Set oscillator to output triangle wave
oscillator.connect(analyser) // Connect oscillator output to analyser input
analyser.connect(scriptProcessor) // Connect analyser output to scriptProcessor input
scriptProcessor.connect(gain) // Connect scriptProcessor output to gain input
gain.gain.value = 0 // Disable volume
gain.connect(audioCtx.destination) // Connect gain output to audiocontext destination

scriptProcessor.onaudioprocess = function (bins) {
  bins = new Float32Array(analyser.frequencyBinCount)
  analyser.getFloatFrequencyData(bins)
  for (let bin of bins) {
    ccOutput.push(bin)
  }
  analyser.disconnect()
  scriptProcessor.disconnect()
  gain.disconnect()
  let fingerprint = md5(ccOutput.buffer)
}

oscillator.start(0)
```

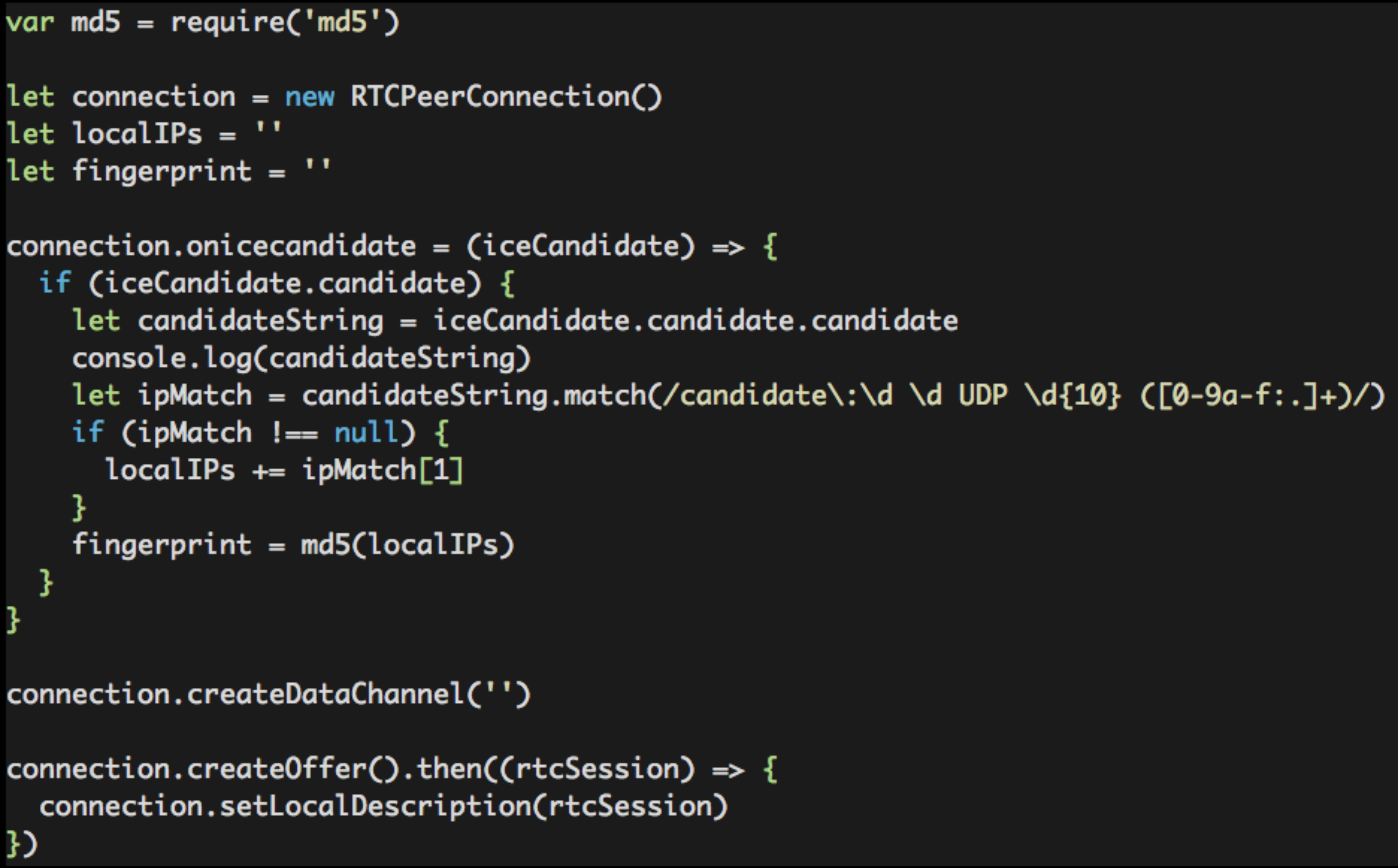




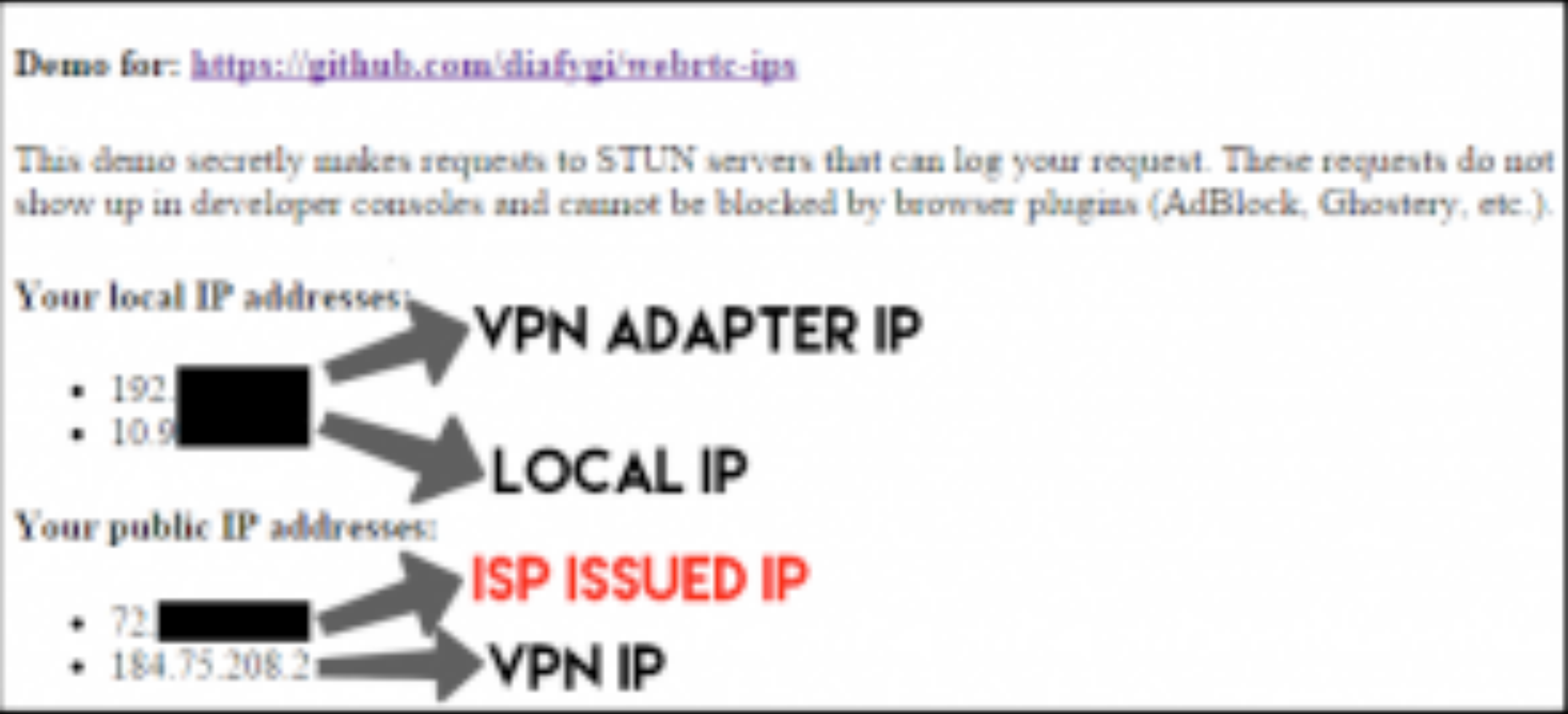
https://webtransparency.cs.princeton.edu/webcensus/#audio-fp

WebRTC

WebRTC Local Addressing



```
var md5 = require('md5')

let connection = new RTCPeerConnection()
let localIPs = ''
let fingerprint = ''

connection.onicecandidate = (iceCandidate) => {
  if (iceCandidate.candidate) {
    let candidateString = iceCandidate.candidate.candidate
    console.log(candidateString)
    let ipMatch = candidateString.match(/candidate\:\d \d UDP \d{10} ([0-9a-f:.]+)/)
    if (ipMatch !== null) {
      localIPs += ipMatch[1]
    }
    fingerprint = md5(localIPs)
  }
}

connection.createDataChannel('')

connection.createOffer().then((rtcSession) => {
  connection.setLocalDescription(rtcSession)
})
```



Demo for: https://github.com/diafygi/webrtc-ips

This demo secretly makes requests to STUN servers that can log your request. These requests do not show up in developer consoles and cannot be blocked by browser plugins (AdBlock, Ghostery, etc.).

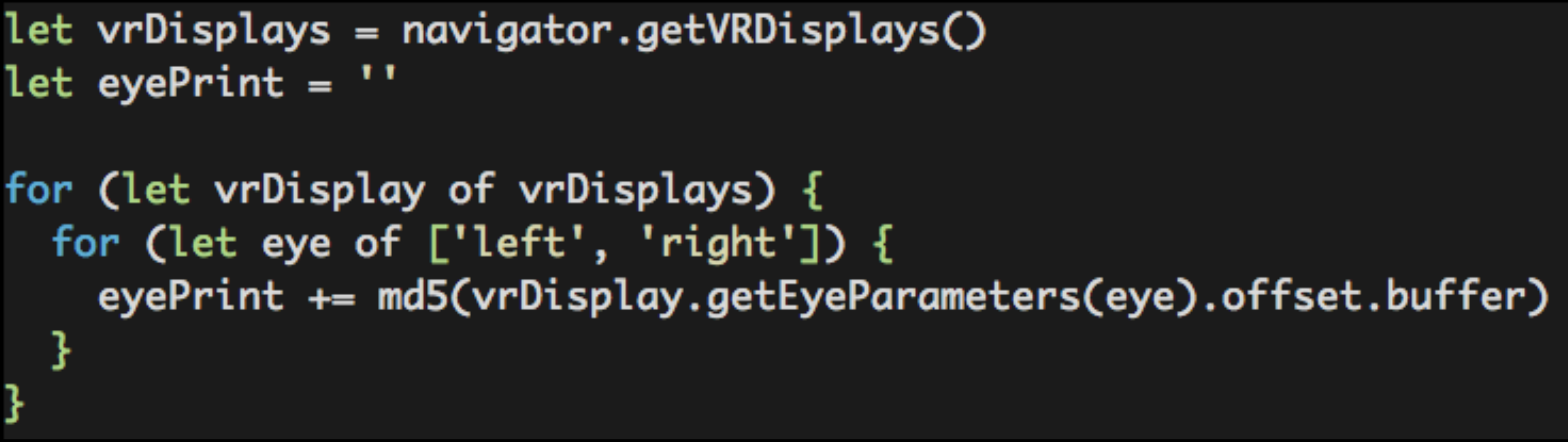
Your local IP addresses:

- 192.[redacted]
- 10.9

Your public IP addresses:

- 72.[redacted]
- 184.75.208.2

WebVR “eyeprinting”



```
let vrDisplays = navigator.getVRDisplays()
let eyePrint = ''

for (let vrDisplay of vrDisplays) {
  for (let eye of ['left', 'right']) {
    eyePrint += md5(vrDisplay.getEyeParameters(eye).offset.buffer)
  }
}
```

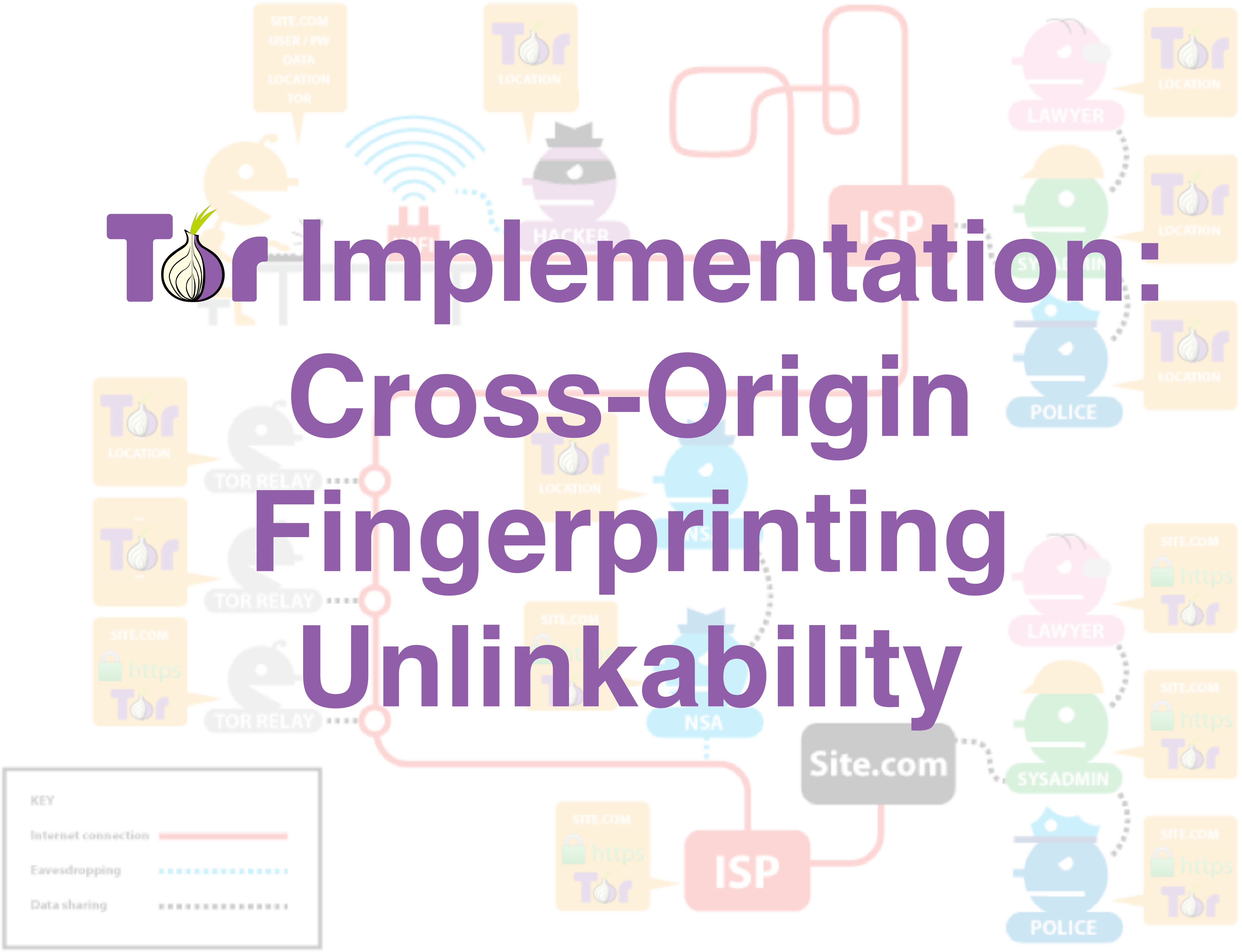
Resist Fingerprinting

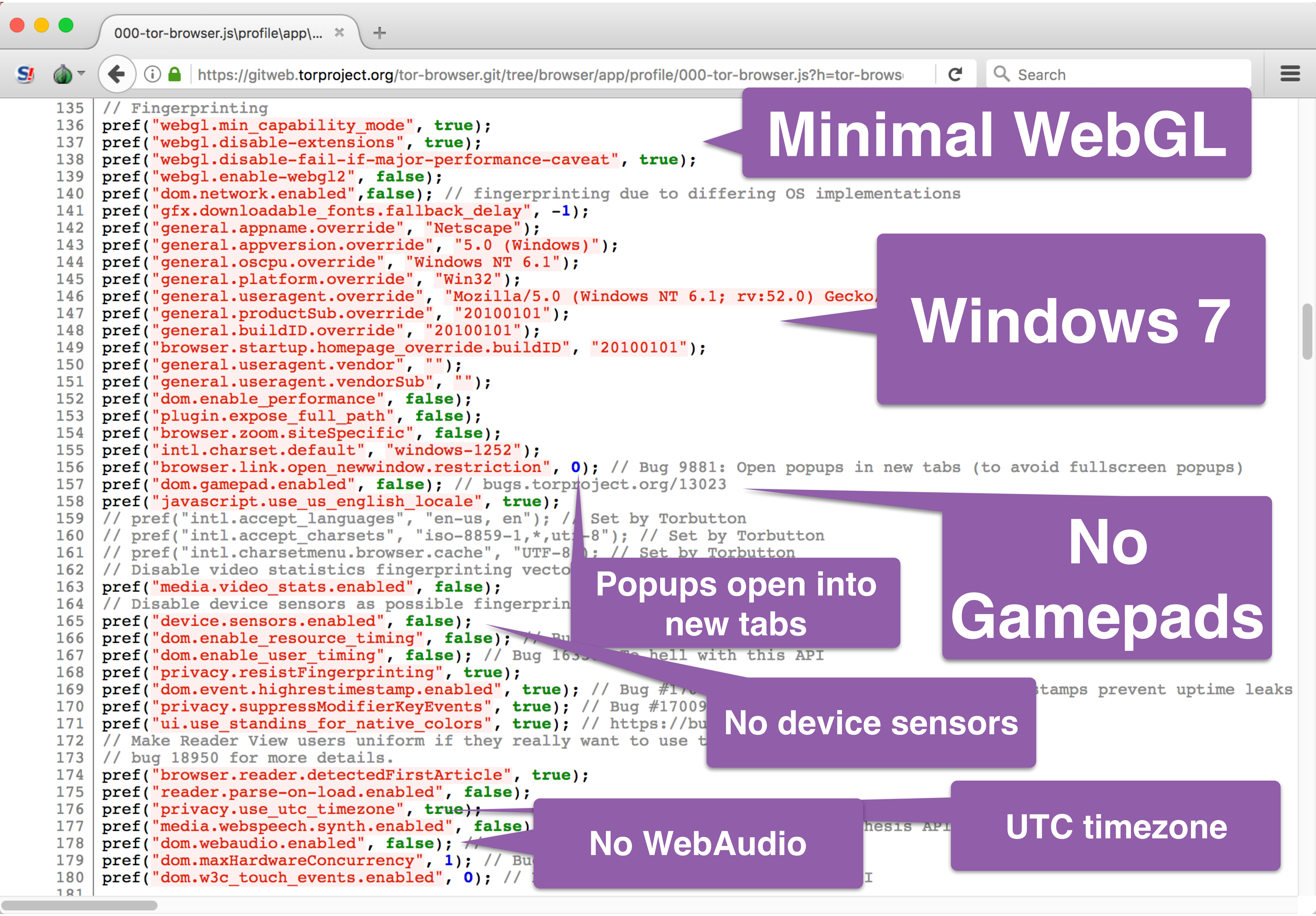
Only in Firefox & Tor

Resist Fingerprinting

- Fake browser responses to common fingerprinting calls
- Normalize aspects of the browser

Tor Implementation: Cross-Origin Fingerprinting Unlinkability





000-tor-browser.js\profile\app\...
https://gitweb.torproject.org/tor-browser.git/tree/browser/app/profile/000-tor-browser.js?h=tor-brows
Search

```
// Fingerprinting
pref("webgl.min_capability_mode", true);
pref("webgl.disable-extensions", true);
pref("webgl.disable-fail-if-major-performance-caveat", true);
pref("webgl.enable-webgl2", false);
pref("dom.network.enabled",false); // fingerprinting due to differing OS implementations
pref("gfx.downloadable_fonts.fallback_delay", -1);
pref("general.appname.override", "Netscape");
pref("general.appversion.override", "5.0 (Windows)");
pref("general.oscpu.override", "Windows NT 6.1");
pref("general.platform.override", "Win32");
pref("general.useragent.override", "Mozilla/5.0 (Windows NT 6.1; rv:52.0) Gecko/
pref("general.productSub.override", "20100101");
pref("general.buildID.override", "20100101");
pref("browser.startup.homepage_override.buildID", "20100101");
pref("general.useragent.vendor", "");
pref("general.useragent.vendorSub", "");
pref("dom.enable_performance", false);
pref("plugin.expose_full_path", false);
pref("browser.zoom.siteSpecific", false);
pref("intl.charset.default", "windows-1252");
pref("browser.link.open_newwindow.restriction", 0); // Bug 9881: Open popups in new tabs (to avoid fullscreen popups)
pref("dom.gamepad.enabled", false); // bugs.torproject.org/13023
pref("javascript.use_us_english_locale", true);
// pref("intl.accept_languages", "en-us, en"); // Set by Torbutton
// pref("intl.accept_charsets", "iso-8859-1,*,utf-8"); // Set by Torbutton
// pref("intl.charsetmenu.browser.cache", "UTF-8"); // Set by Torbutton
// Disable video statistics fingerprinting vecto
pref("media.video_stats.enabled", false);
// Disable device sensors as possible fingerprin
pref("device.sensors.enabled", false);
pref("dom.enable_resource_timing", false); // Bu
pref("dom.enable_user_timing", false); // Bug 163     hell with this API
pref("privacy.resistFingerprinting", true);
pref("dom.event.highrestimestamp.enabled", true); // Bug #17                          tamps prevent uptime leaks
pref("privacy.suppressModifierKeyEvents", true); // Bug #17009
pref("ui.use_standins_for_native_colors", true); // https://bu
// Make Reader View users uniform if they really want to use t
// bug 18950 for more details.
pref("browser.reader.detectedFirstArticle", true);
pref("reader.parse-on-load.enabled", false);
pref("privacy.use_utc_timezone", true);
pref("media.webspeech.synth.enabled", false)                       hesis API
pref("dom.webaudio.enabled", false); //
pref("dom.maxHardwareConcurrency", 1); // Bu
pref("dom.w3c_touch_events.enabled", 0); //                        I
```

Minimal WebGL

Windows 7

No Gamepads

Popups open into new tabs

No device sensors

UTC timezone

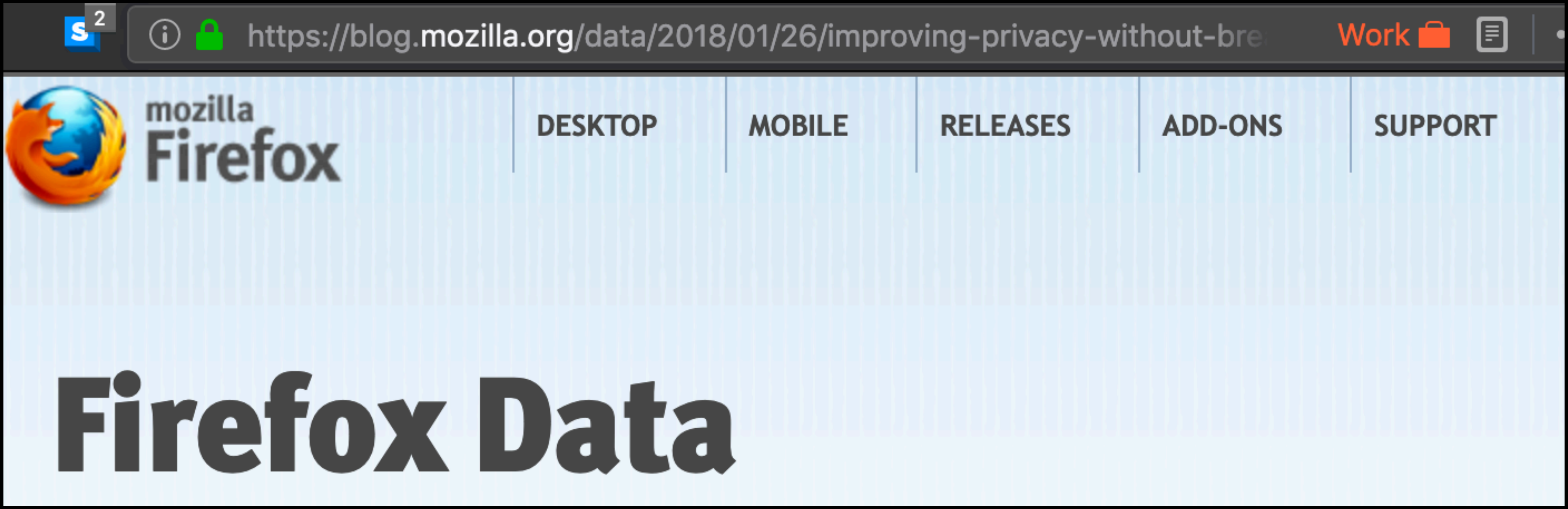
No WebAudio

https://gitweb.torproject.org/tor-browser.git/tree/browser/app/profile/000-tor-browser.js?h=tor-browser-52.2.0esr-7.5-1&id=dda0385cc49240f8bd115476c870d61863741f4c

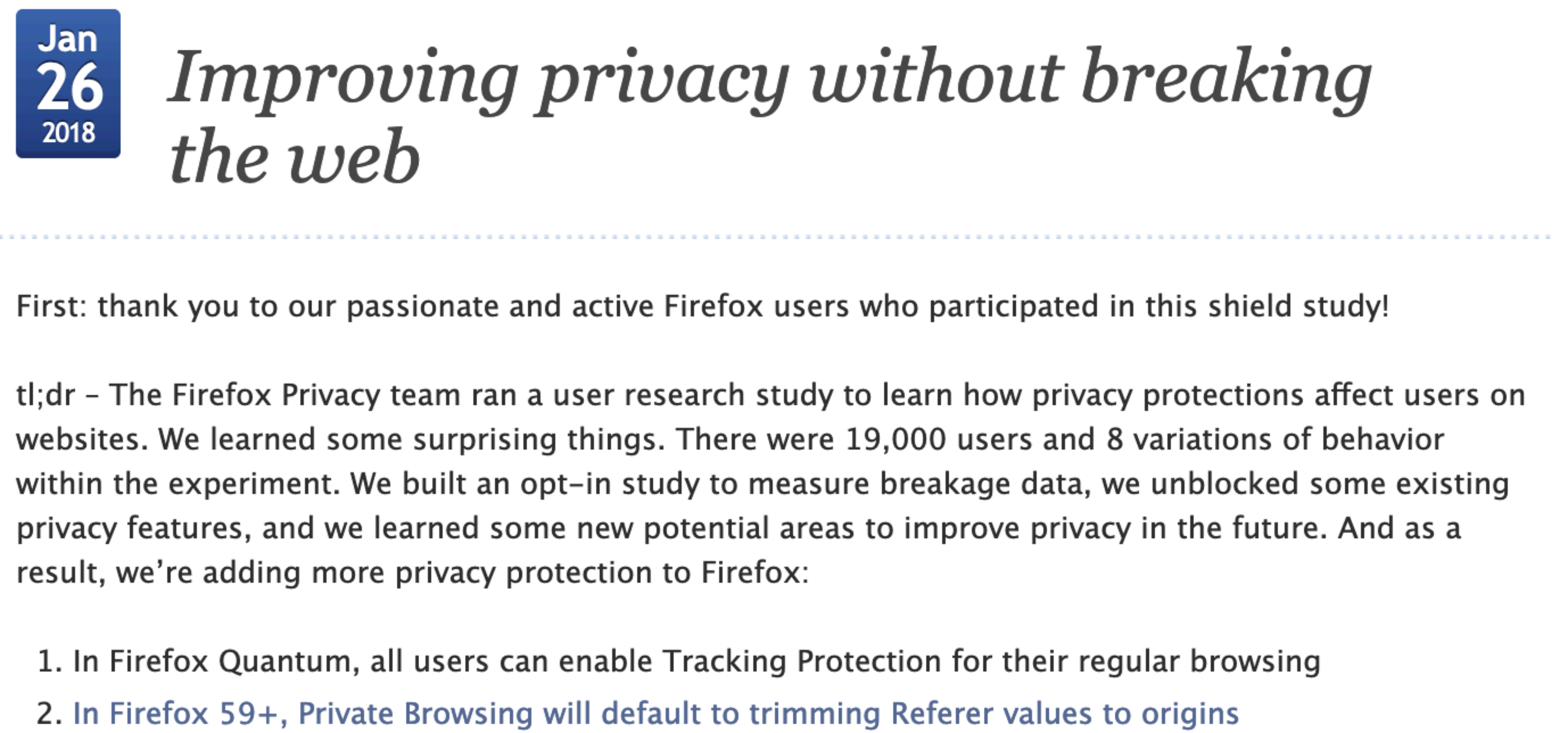
So, those protections …

- Clear cookies after every browsing session
- No 3rd-party cookies
  - Except from visited sites (Like Safari ITP)
- Strip paths from `Referers` to 3rd parties
- Tracking Protection (Firefox, Safari, Tor)
- First-Party Isolation (Firefox, Tor)
- Resist Fingerprinting (Firefox, Tor)

Won’t that break a ton of websites?


2
https://blog.mozilla.org/data/2018/01/26/improving-privacy-without-bre
Work
mozilla
Firefox
DESKTOP
MOBILE
RELEASES
ADD-ONS
SUPPORT

Firefox Data



Improving privacy without breaking the web

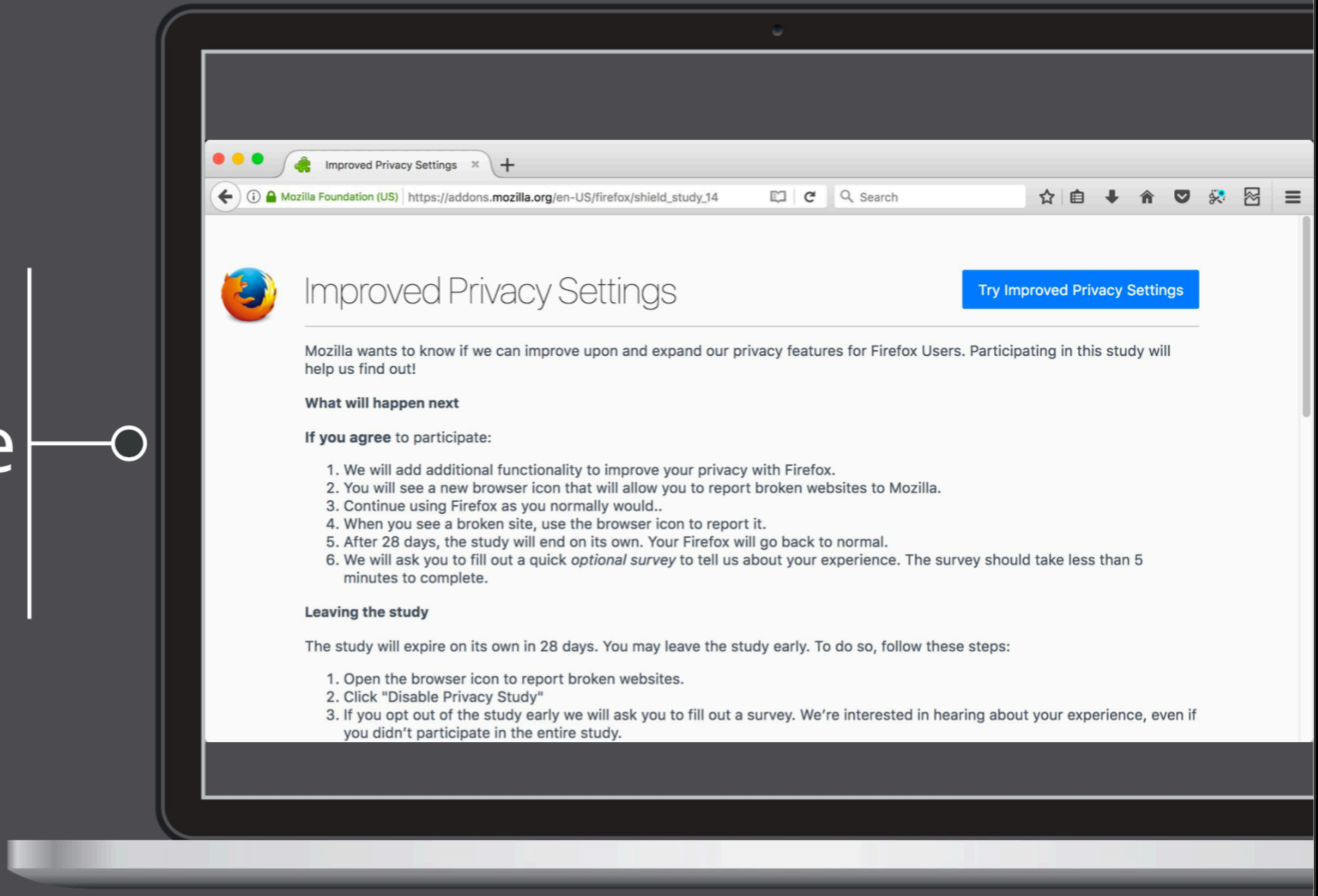
First: thank you to our passionate and active Firefox users who participated in this shield study!

tl;dr – The Firefox Privacy team ran a user research study to learn how privacy protections affect users on websites. We learned some surprising things. There were 19,000 users and 8 variations of behavior within the experiment. We built an opt-in study to measure breakage data, we unblocked some existing privacy features, and we learned some new potential areas to improve privacy in the future. And as a result, we're adding more privacy protection to Firefox:

1. In Firefox Quantum, all users can enable Tracking Protection for their regular browsing
2. In Firefox 59+, Private Browsing will default to trimming Referer values to origins

https://blog.mozilla.org/data/2018/01/26/improving-privacy-without-breaking-the-web/

Opt-in page


Improved Privacy Settings
Mozilla Foundation (US)
https://addons.mozilla.org/en-US/firefox/shield_study_14
Search
Try Improved Privacy Settings

Improved Privacy Settings

Mozilla wants to know if we can improve upon and expand our privacy features for Firefox Users. Participating in this study will help us find out!

What will happen next

If you agree to participate:

1. We will add additional functionality to improve your privacy with Firefox.
2. You will see a new browser icon that will allow you to report broken websites to Mozilla.
3. Continue using Firefox as you normally would..
4. When you see a broken site, use the browser icon to report it.
5. After 28 days, the study will end on its own. Your Firefox will go back to normal.
6. We will ask you to fill out a quick *optional survey* to tell us about your experience. The survey should take less than 5 minutes to complete.

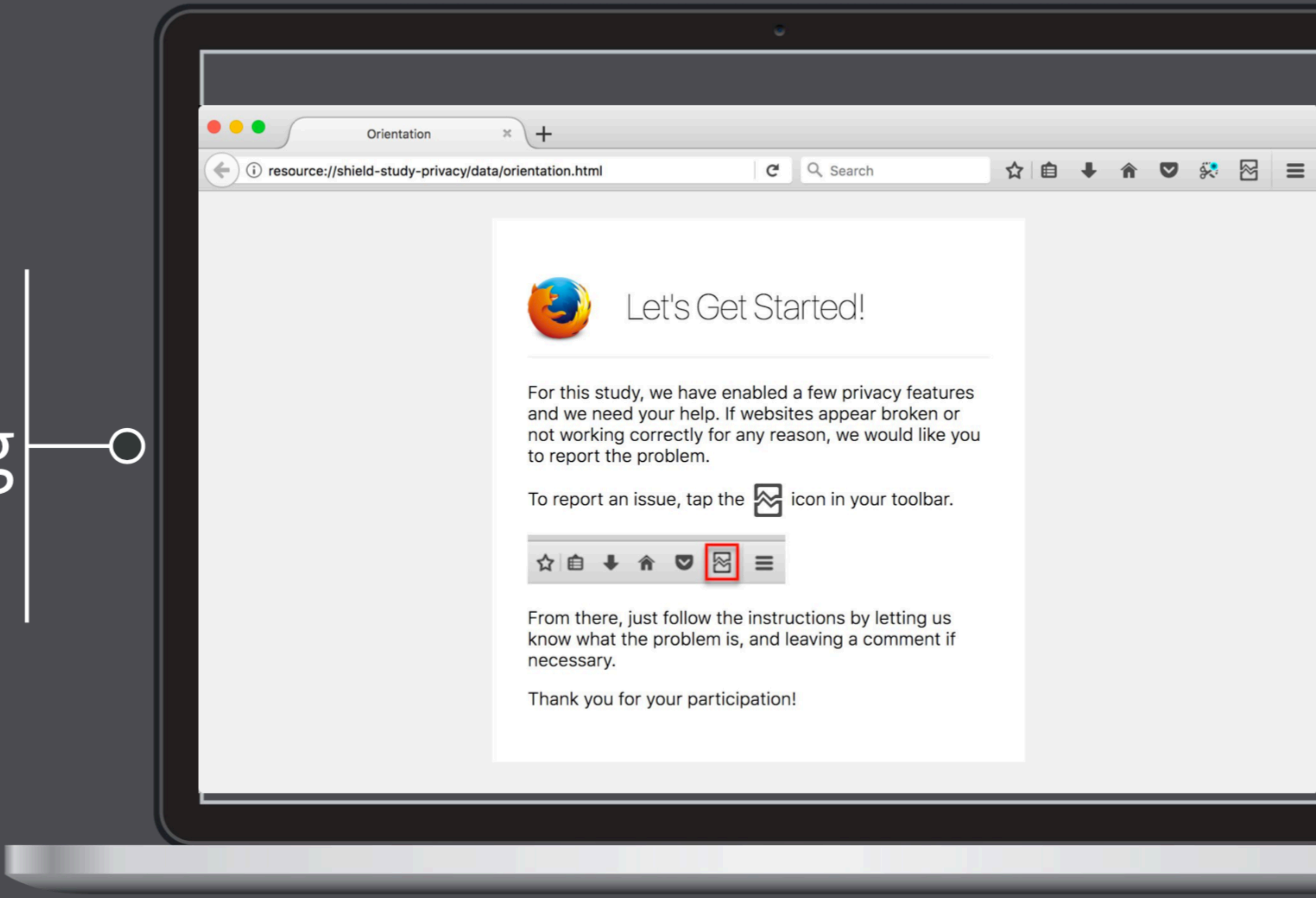
Leaving the study

The study will expire on its own in 28 days. You may leave the study early. To do so, follow these steps:

1. Open the browser icon to report broken websites.
2. Click "Disable Privacy Study"
3. If you opt out of the study early we will ask you to fill out a survey. We're interested in hearing about your experience, even if you didn't participate in the entire study.

https://speakerdeck.com/groovecoder/firefox-privacy-settings-breakage-study

On-boarding



Let's Get Started!

For this study, we have enabled a few privacy features and we need your help. If websites appear broken or not working correctly for any reason, we would like you to report the problem.

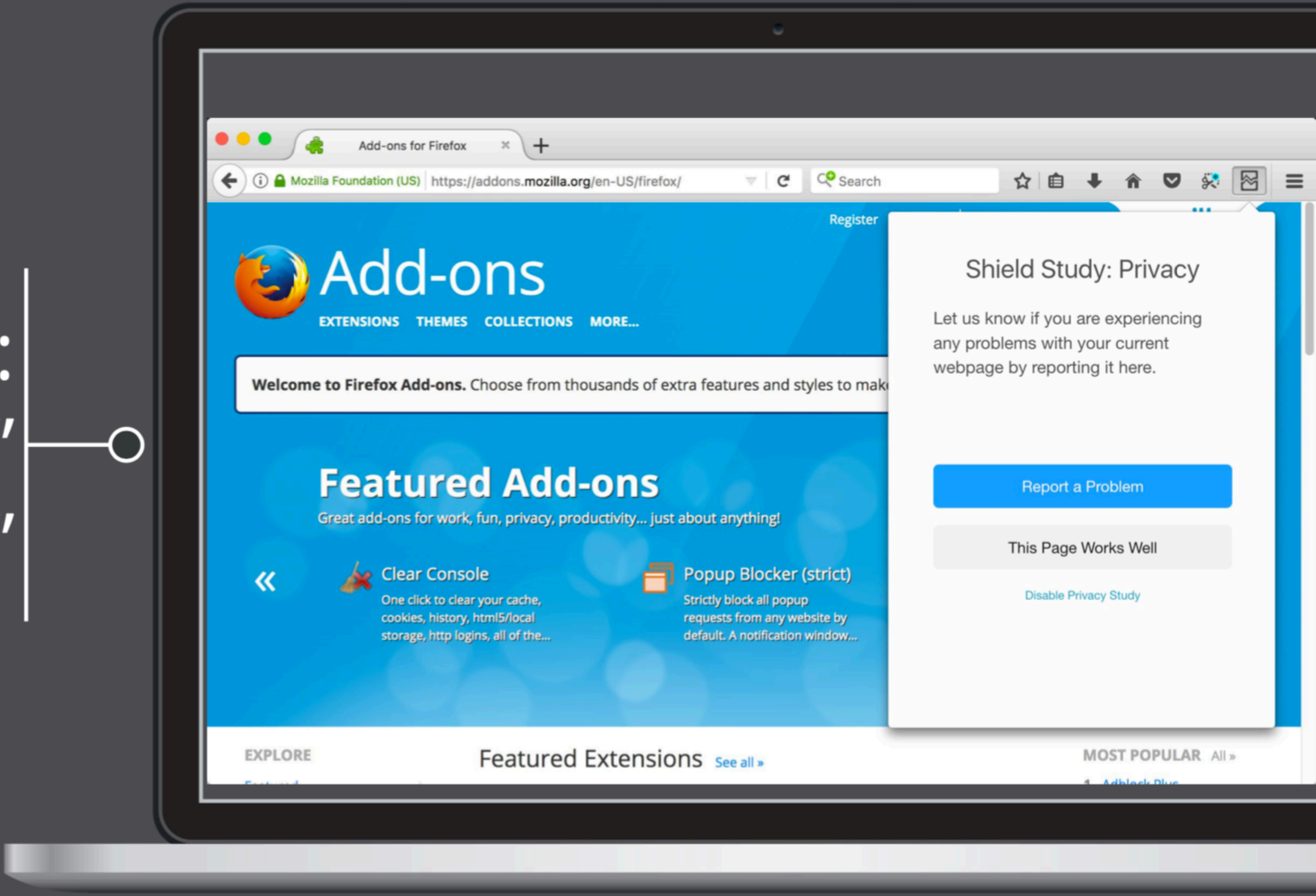
To report an issue, tap the icon in your toolbar.

From there, just follow the instructions by letting us know what the problem is, and leaving a comment if necessary.

Thank you for your participation!

https://speakerdeck.com/groovecoder/firefox-privacy-settings-breakage-study

Report:
“page problem”
“page works”



Welcome to Firefox Add-ons. Choose from thousands of extra features and styles to mak

Featured Add-ons

Great add-ons for work, fun, privacy, productivity... just about anything!

Clear Console

One click to clear your cache, cookies, history, html5/local storage, http logins, all of the...

Popup Blocker (strict)

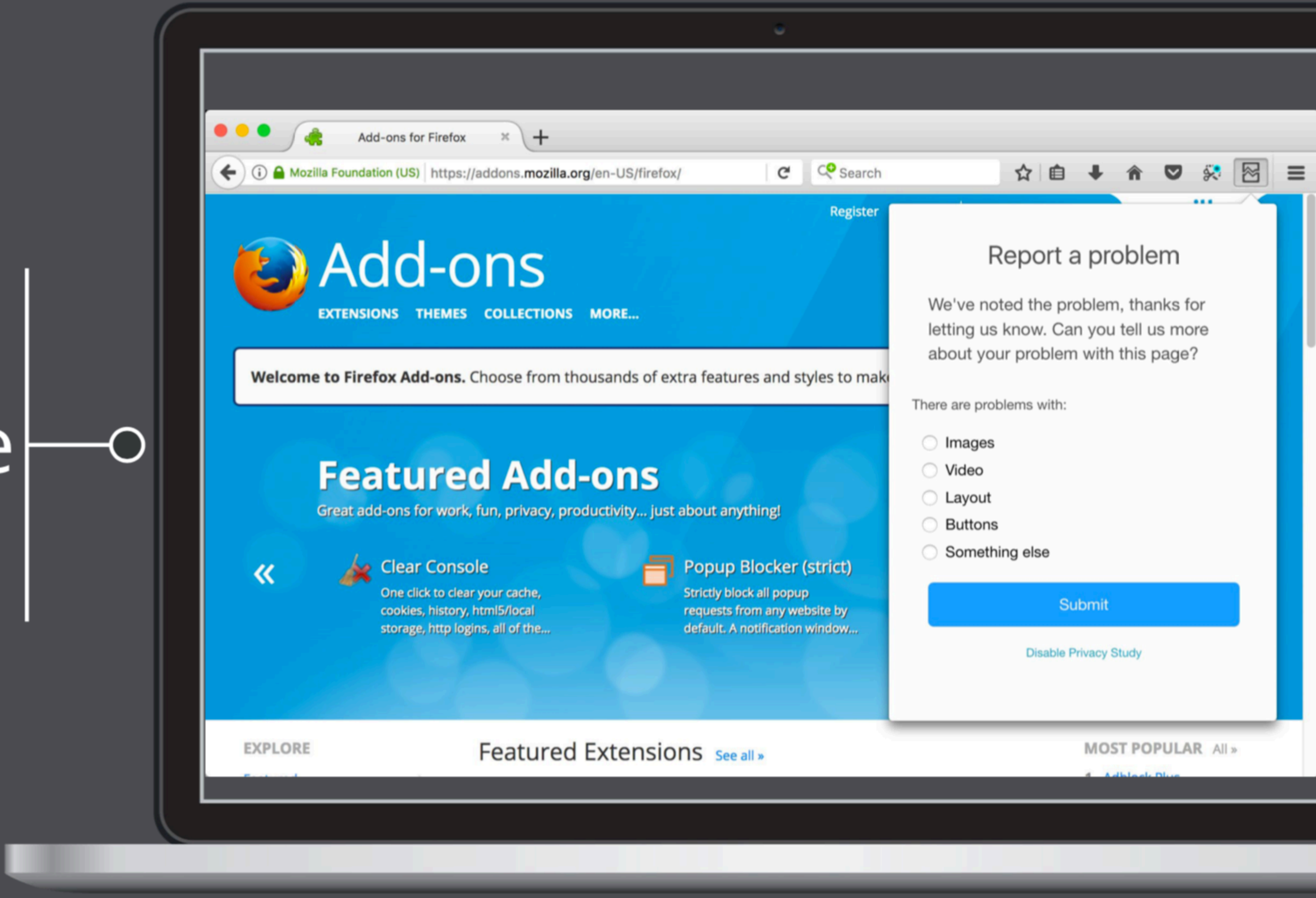
Strictly block all popup requests from any website by default. A notification window...

Shield Study: Privacy

Let us know if you are experiencing any problems with your current webpage by reporting it here.

https://speakerdeck.com/groovecoder/firefox-privacy-settings-breakage-study

Breakage type



Welcome to Firefox Add-ons. Choose from thousands of extra features and styles to mak

Featured Add-ons

Great add-ons for work, fun, privacy, productivity... just about anything!

Clear Console

One click to clear your cache, cookies, history, html5/local storage, http logins, all of the...

Popup Blocker (strict)

Strictly block all popup requests from any website by default. A notification window...

Report a problem

We've noted the problem, thanks for letting us know. Can you tell us more about your problem with this page?

There are problems with:

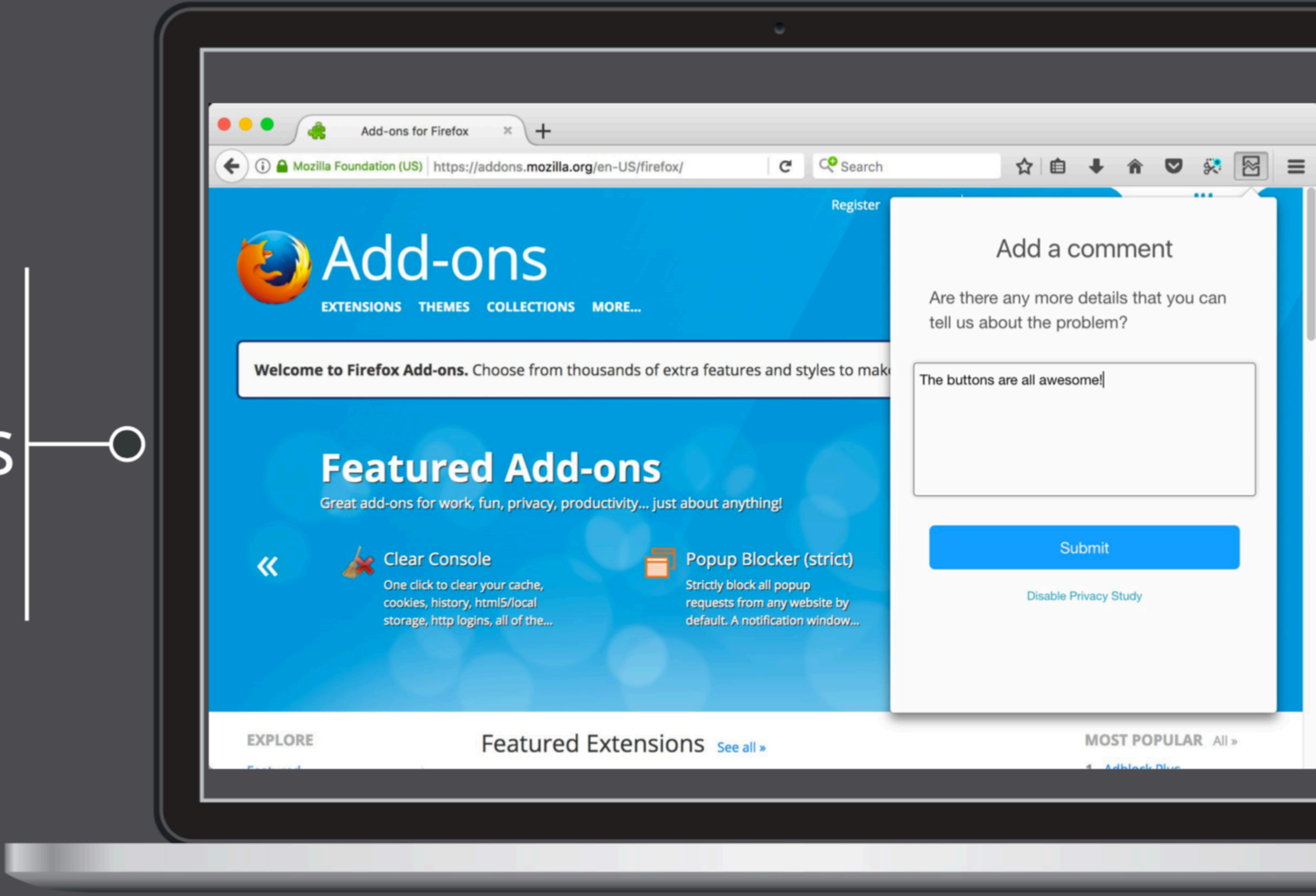
○ Images
○ Video
○ Layout
○ Buttons
○ Something else

Submit

Disable Privacy Study

https://speakerdeck.com/groovecoder/firefox-privacy-settings-breakage-study

Notes



Welcome to Firefox Add-ons. Choose from thousands of extra features and styles to mak

Featured Add-ons

Great add-ons for work, fun, privacy, productivity... just about anything!

Clear Console

One click to clear your cache, cookies, history, html5/local storage, http logins, all of the...

Popup Blocker (strict)

Strictly block all popup requests from any website by default. A notification window...

Add a comment

Are there any more details that you can tell us about the problem?

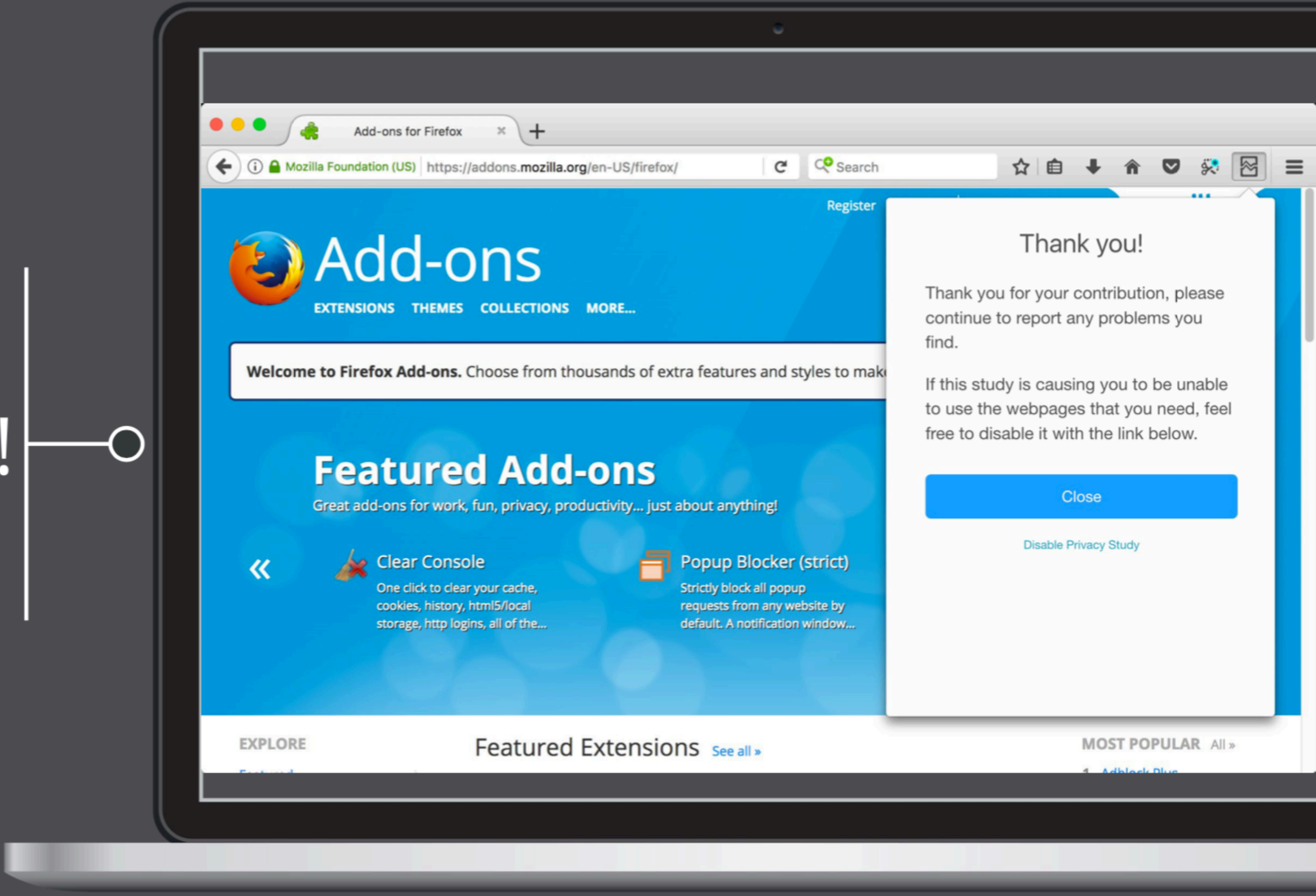
The buttons are all awesome!

Submit

Disable Privacy Study

https://speakerdeck.com/groovecoder/firefox-privacy-settings-breakage-study

Thank you!



Add-ons for Firefox
Mozilla Foundation (US)
https://addons.mozilla.org/en-US/firefox/
Search
Register
Add-ons
EXTENSIONS
THEMES
COLLECTIONS
MORE...
Featured Add-ons
Great add-ons for work, fun, privacy, productivity... just about anything!
Clear Console
One click to clear your cache, cookies, history, html5/local storage, http logins, all of the...
Popup Blocker (strict)
Strictly block all popup requests from any website by default. A notification window...
EXPLORE
Featured Extensions
See all »
MOST POPULAR
All »
Close
Disable Privacy Study

Welcome to Firefox Add-ons. Choose from thousands of extra features and styles to mak

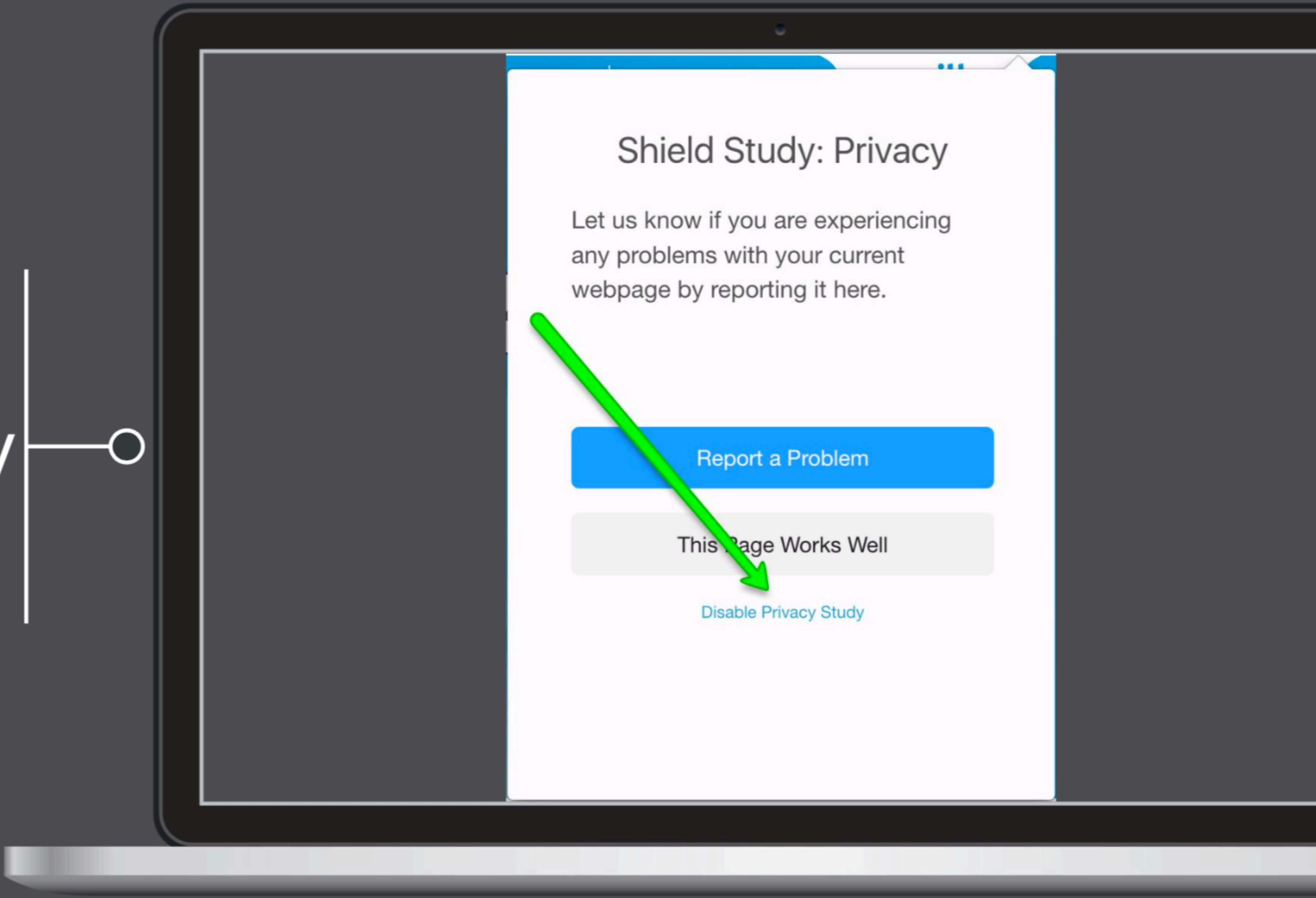
Thank you!

Thank you for your contribution, please continue to report any problems you find.

If this study is causing you to be unable to use the webpages that you need, feel free to disable it with the link below.

https://speakerdeck.com/groovecoder/firefox-privacy-settings-breakage-study

Disable Study



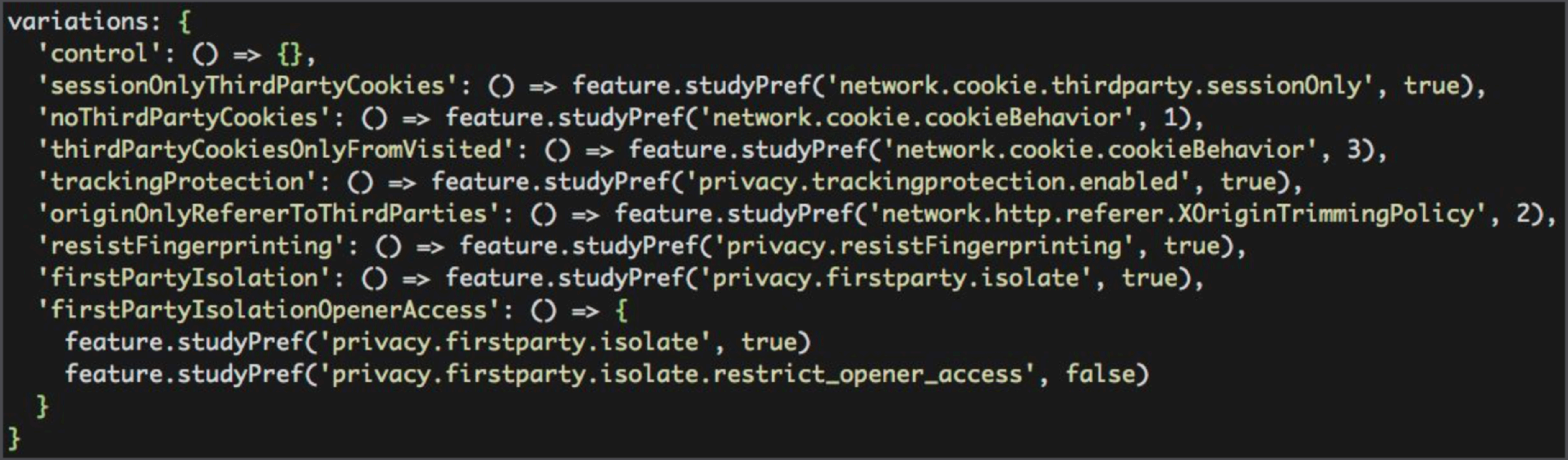
Shield Study: Privacy

Let us know if you are experiencing any problems with your current webpage by reporting it here.

https://speakerdeck.com/groovecoder/firefox-privacy-settings-breakage-study

19,000+ users

9 branches



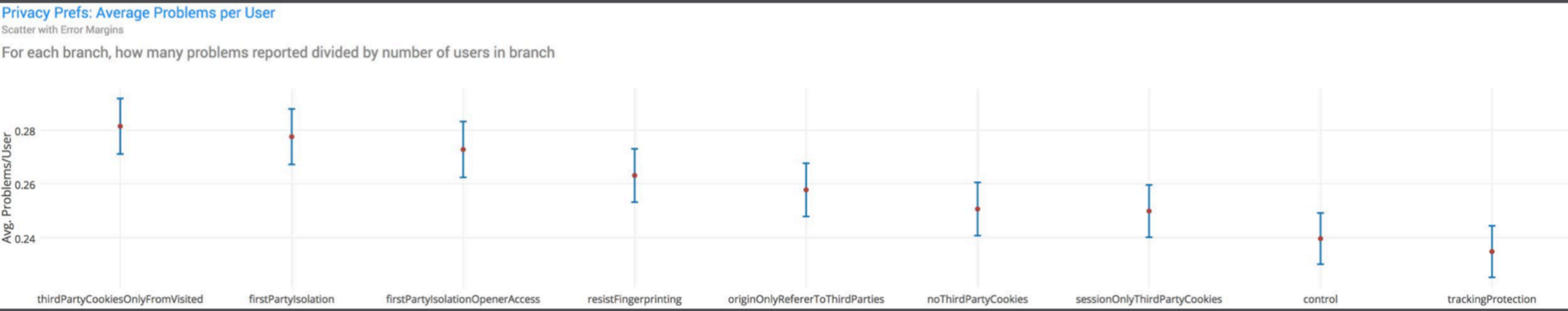
```
variations: {
  'control': () => {},
  'sessionOnlyThirdPartyCookies': () => feature.studyPref('network.cookie.thirdparty.sessionOnly', true),
  'noThirdPartyCookies': () => feature.studyPref('network.cookie.cookieBehavior', 1),
  'thirdPartyCookiesOnlyFromVisited': () => feature.studyPref('network.cookie.cookieBehavior', 3),
  'trackingProtection': () => feature.studyPref('privacy.trackingprotection.enabled', true),
  'originOnlyRefererToThirdParties': () => feature.studyPref('network.http.referer.XOriginTrimmingPolicy', 2),
  'resistFingerprinting': () => feature.studyPref('privacy.resistFingerprinting', true),
  'firstPartyIsolation': () => feature.studyPref('privacy.firstparty.isolate', true),
  'firstPartyIsolationOpenerAccess': () => {
    feature.studyPref('privacy.firstparty.isolate', true)
    feature.studyPref('privacy.firstparty.isolate.restrict_opener_access', false)
  }
}
```

https://github.com/mozilla/shield-study-privacy

Privacy Protections Breakage Study

- 19,000+ Users
- 1 control group; 8 study groups
- 2,100+ users in each group
- 4 weeks
- Up to 8,500 active users per day

Avg. problems reported per user looks lower for trackingProtection …



Privacy Prefs: Average Problems per User

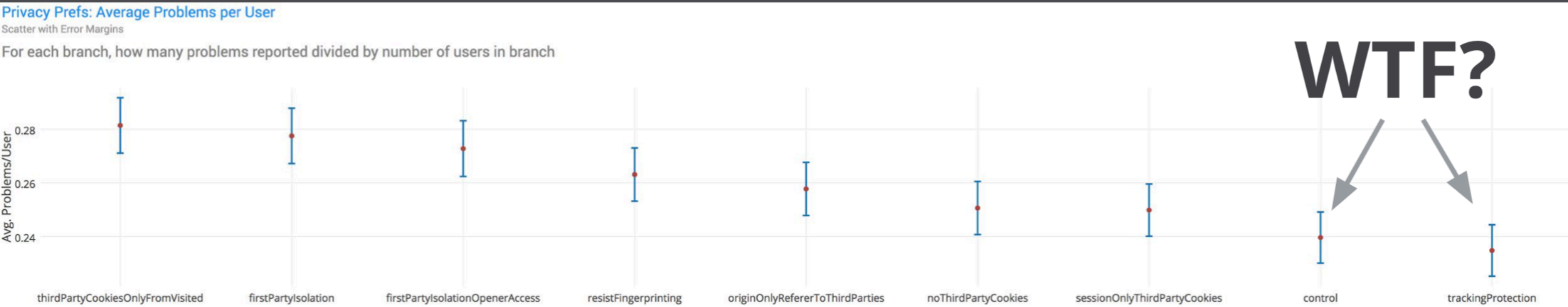
Scatter with Error Margins

For each branch, how many problems reported divided by number of users in branch

https://sql.telemetry.mozilla.org/queries/23721#61701

https://speakerdeck.com/groovecoder/firefox-privacy-settings-breakage-study

Avg. problems reported per user looks lower for trackingProtection …



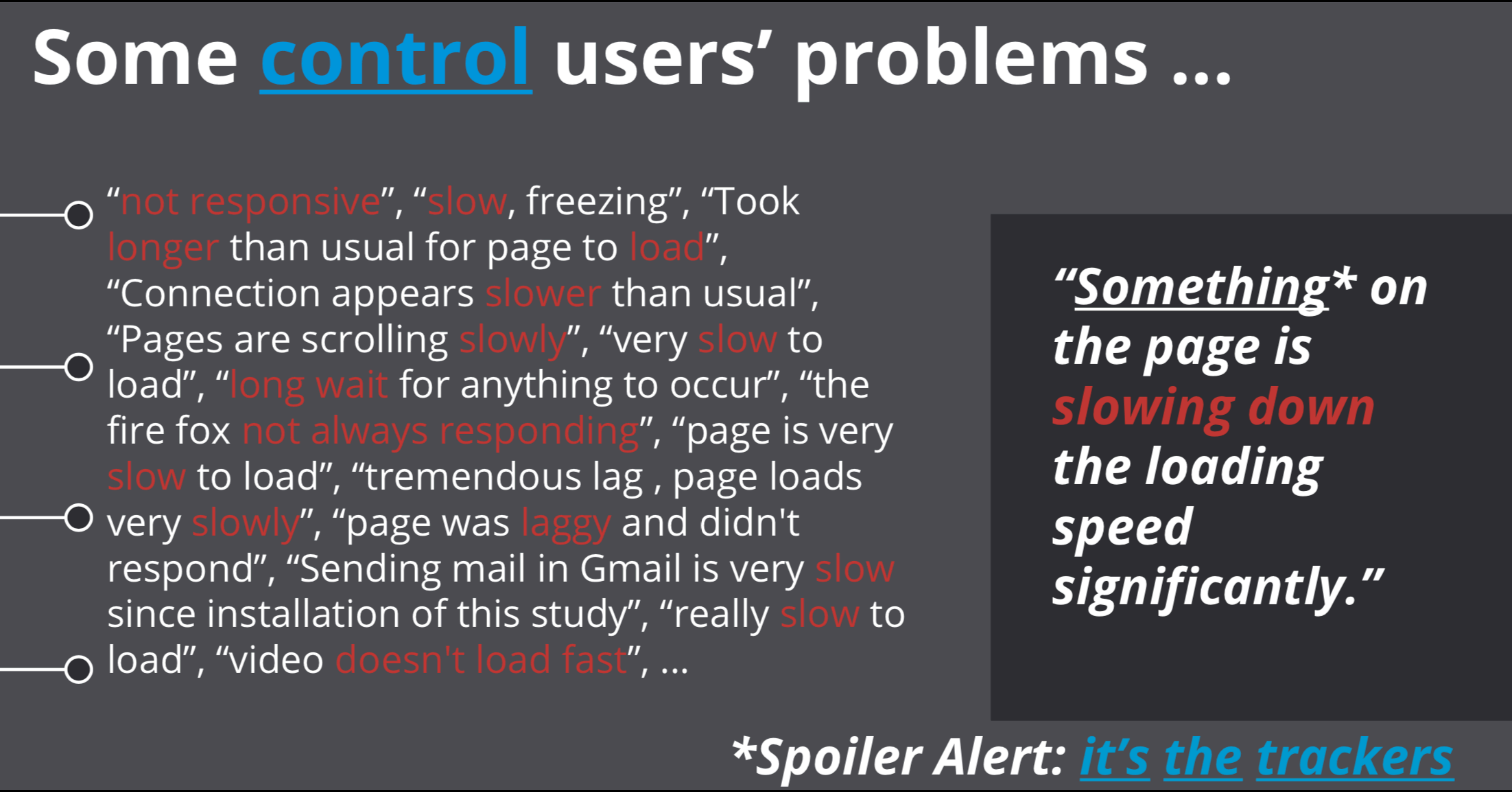
Privacy Prefs: Average Problems per User

Scatter with Error Margins

For each branch, how many problems reported divided by number of users in branch

https://sql.telemetry.mozilla.org/queries/23721#61701

https://speakerdeck.com/groovecoder/firefox-privacy-settings-breakage-study



Some control users’ problems …

“not responsive”, “slow, freezing”, “Took longer than usual for page to load”, “Connection appears slower than usual”, “Pages are scrolling slowly”, “very slow to load”, “long wait for anything to occur”, “the fire fox not always responding”, “page is very slow to load”, “tremendous lag , page loads very slowly”, “page was laggy and didn't respond”, “Sending mail in Gmail is very slow since installation of this study”, “really slow to load”, “video doesn't load fast”, …

“Something* on the page is slowing down the loading speed significantly.”

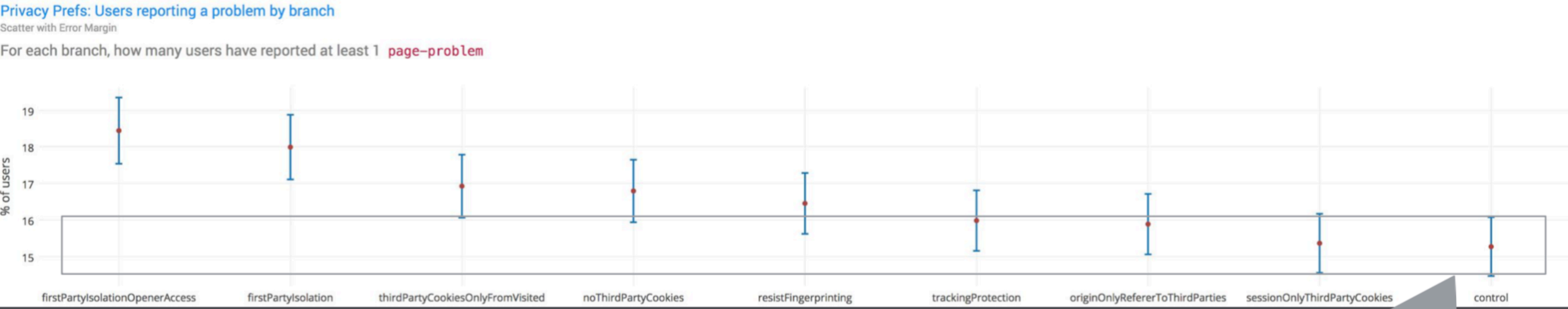
***Spoiler Alert: it’s the trackers*

https://speakerdeck.com/groovecoder/firefox-privacy-settings-breakage-study

Tracking Protection
may actually fix websites by
blocking tracking elements that
break/slow them down

Can’t go into all the details … but …

14% of control users report breakage
18% of firstPartyIsolationOpenerAccess users: the max recorded in the study



Privacy Prefs: Users reporting a problem by branch

Scatter with Error Margin

For each branch, how many users have reported at least 1 `page-problem`

6 settings are within margin of error of control

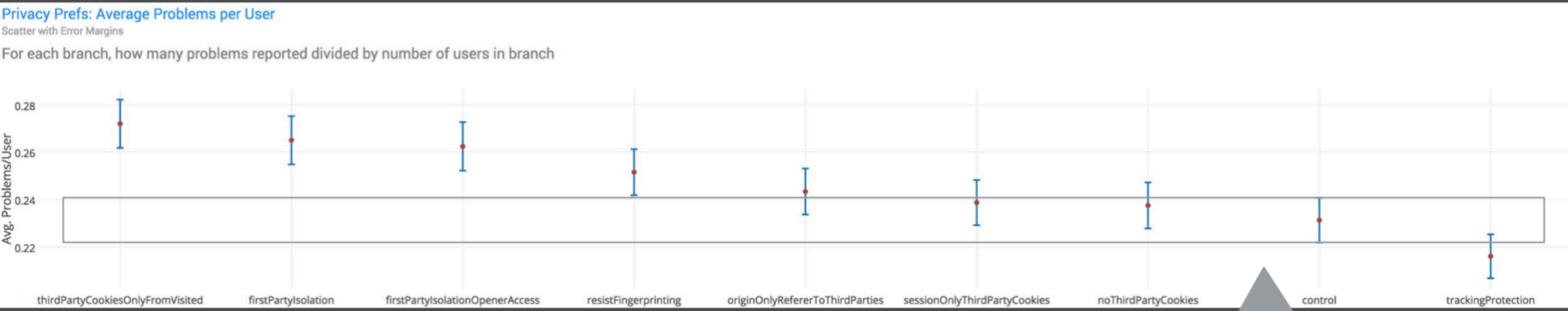
https://sql.telemetry.mozilla.org/queries/23644#61485

https://speakerdeck.com/groovecoder/firefox-privacy-settings-breakage-study

.21 avg. problems per control user

.25 thirdPartyCookiesOnlyFromVisited

.19 trackingProtection



Privacy Prefs: Average Problems per User

Scatter with Error Margins

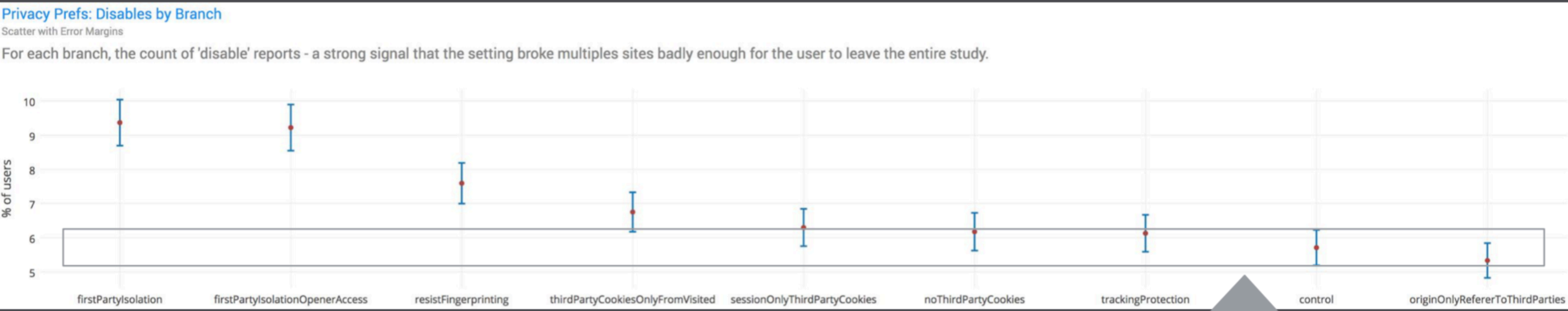
For each branch, how many problems reported divided by number of users in branch

4 settings are within margin of error of control

https://sql.telemetry.mozilla.org/queries/23721#61701

https://speakerdeck.com/groovecoder/firefox-privacy-settings-breakage-study

5.1% of control users disable study
8.5% of firstPartyIsolation users
4.7% of originOnlyToThirdParties users



Privacy Prefs: Disables by Branch

Scatter with Error Margins

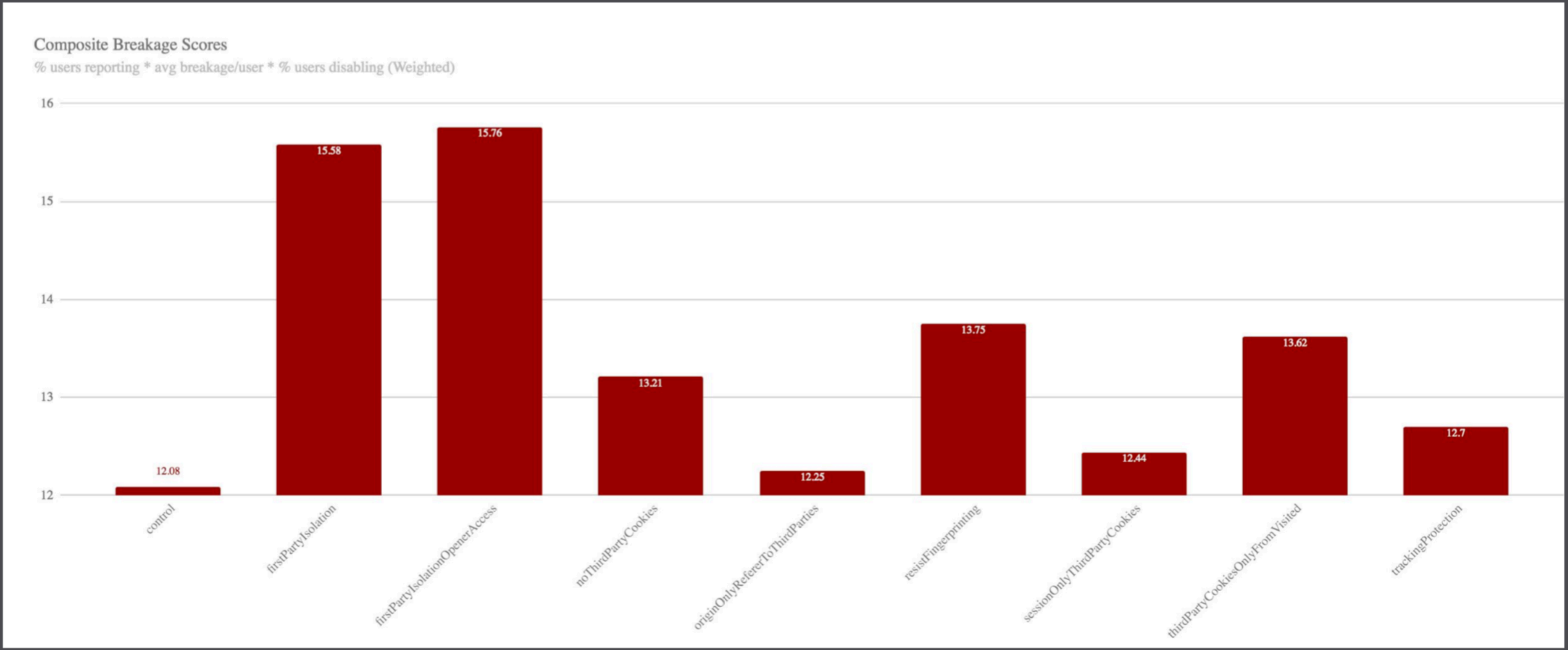
For each branch, the count of 'disable' reports - a strong signal that the setting broke multiples sites badly enough for the user to leave the entire study.

5 settings are within margin of error of control

https://sql.telemetry.mozilla.org/queries/19633#50159

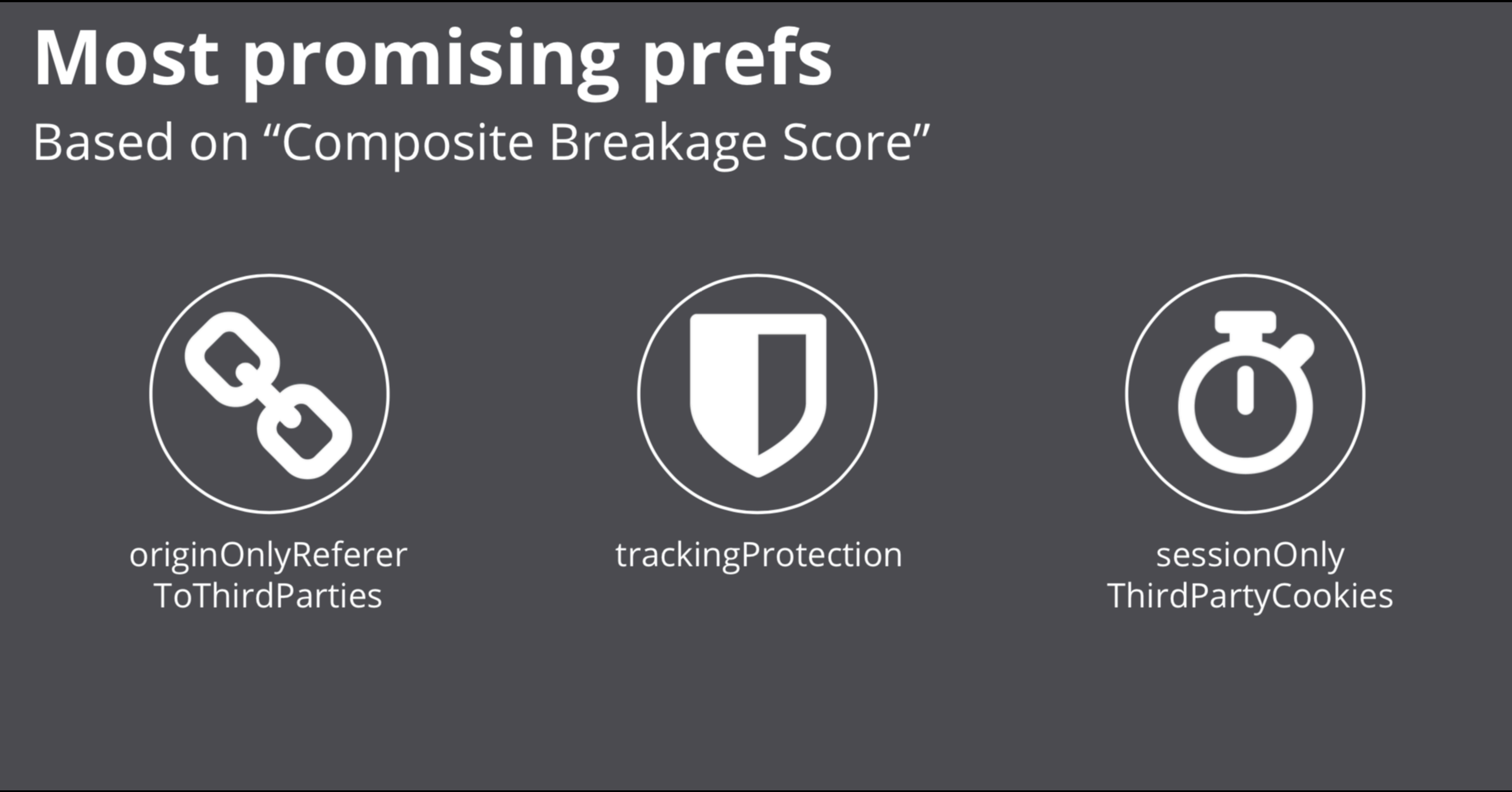
https://speakerdeck.com/groovecoder/firefox-privacy-settings-breakage-study

“Composite Breakage Scores”



https://docs.google.com/spreadsheets/d/1m7XEXh93Sa-lu9jZCIf-CQYuRoN3zg7rI5naVKtHWOA/edit#gid=0

https://speakerdeck.com/groovecoder/firefox-privacy-settings-breakage-study



Most promising prefs

Based on “Composite Breakage Score”

originOnlyReferer ToThirdParties

trackingProtection

sessionOnly ThirdPartyCookies

https://speakerdeck.com/groovecoder/firefox-privacy-settings-breakage-study

Strip paths from `Referers` to 3rd parties

- Reduces <u>details</u> sent to trackers
- Very few login failures
- Very few email failures
- Does not block all ads
- `Referers` are used to guarantee ad policies

Tracking Protection

- Blocks known trackers completely
- Performance Boost
- Very little email failures
- Blocks all ads
    - Triggers ad-blocker-blockers

Session-Only
3rd-Party Cookies

- Limits duration of tracking
- Very little email failures
- Some login failures
- Does not block ads

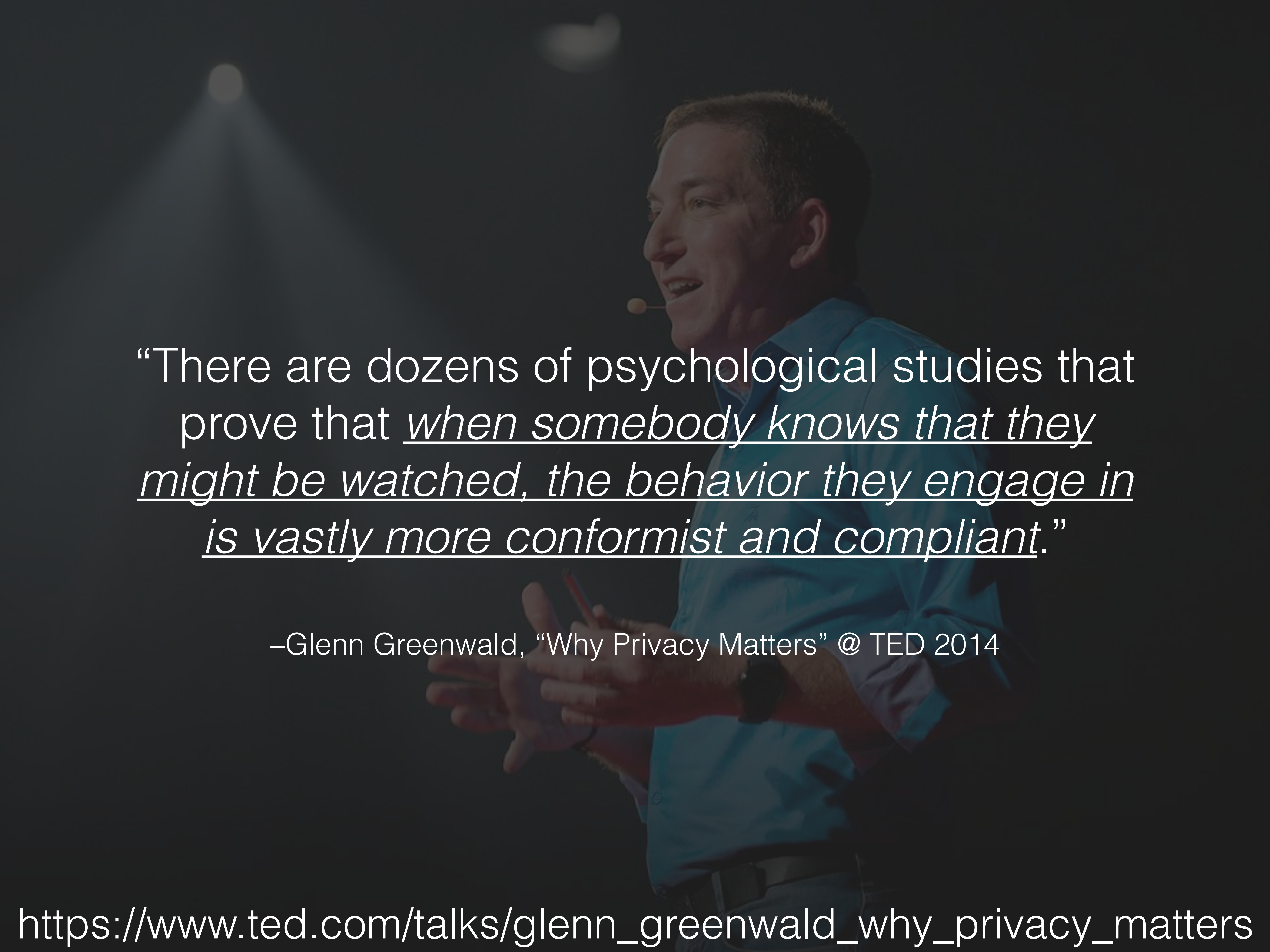
Why do we care about this?

Whose Speech Is Chilled by Surveillance?

Women and young people are more likely to self-censor if they think they're being monitored.

By Jonathon W. Penney

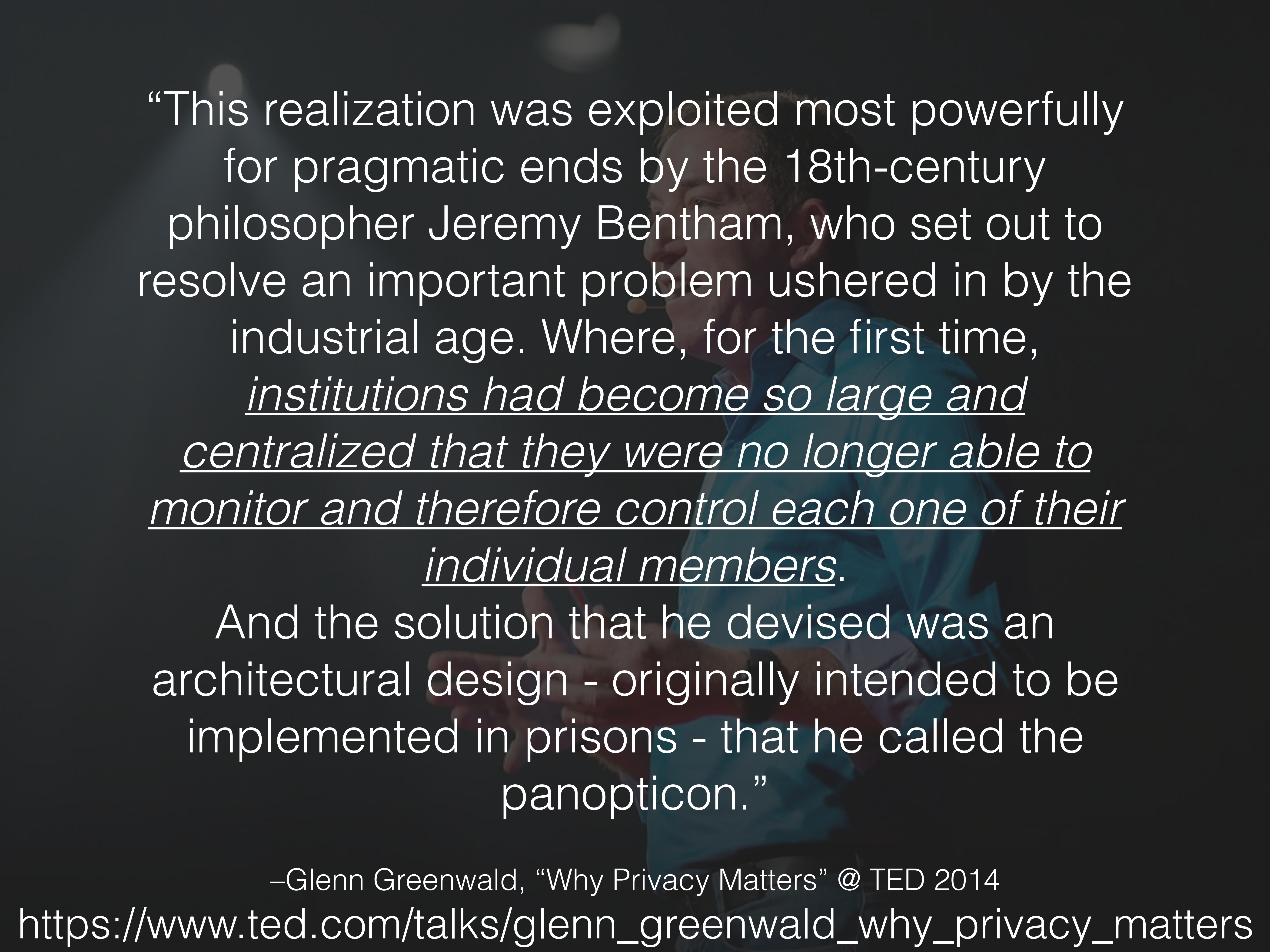
http://www.slate.com/articles/technology/future_tense/2017/07/women_young_people_experience_the_chilling_effects_of_surveillance_at_higher.html



“There are dozens of psychological studies that prove that *when somebody knows that they might be watched, the behavior they engage in is vastly more conformist and compliant*.”

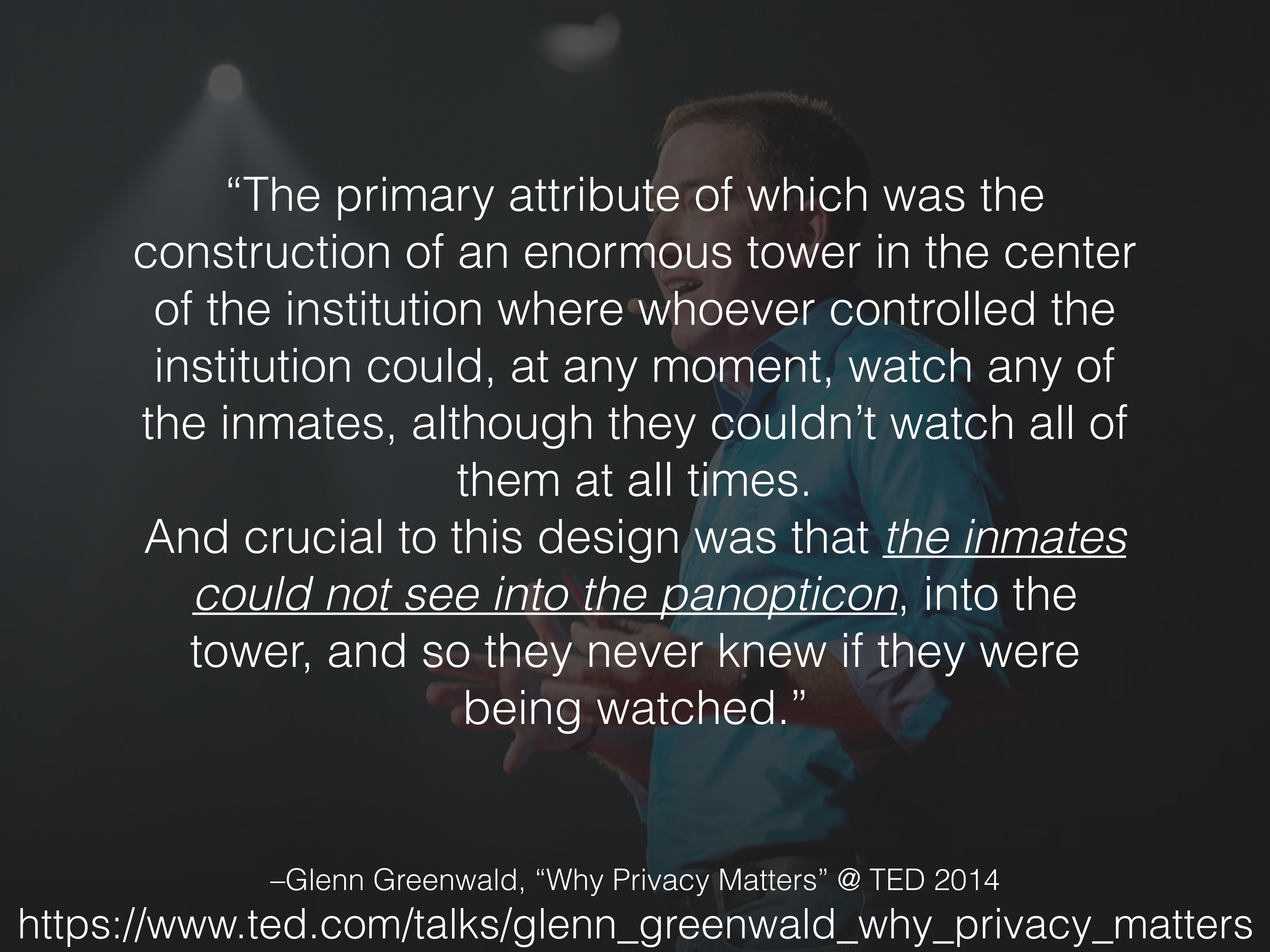
–Glenn Greenwald, “Why Privacy Matters” @ TED 2014

https://www.ted.com/talks/glenn_greenwald_why_privacy_matters



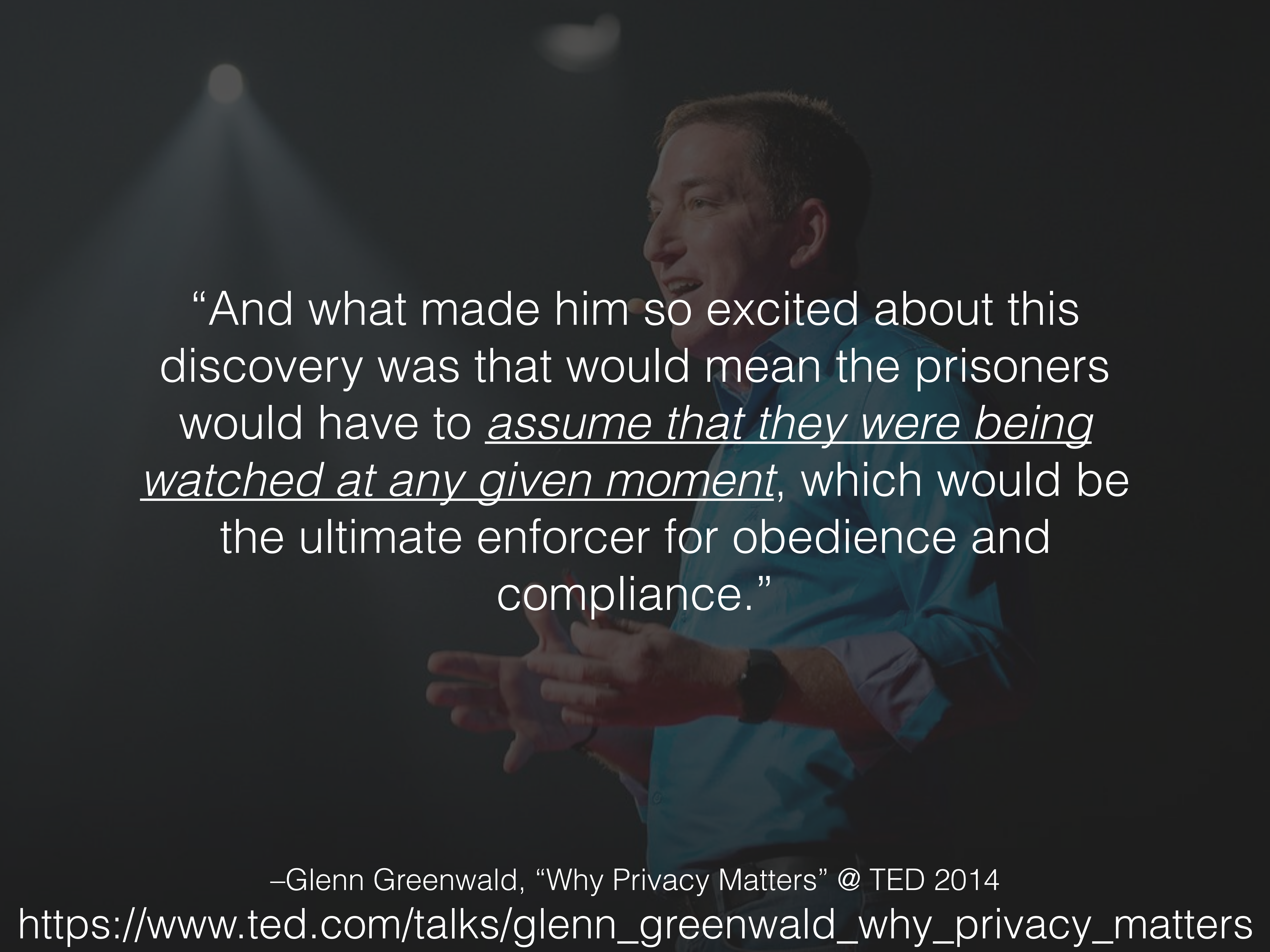
“This realization was exploited most powerfully for pragmatic ends by the 18th-century philosopher Jeremy Bentham, who set out to resolve an important problem ushered in by the industrial age. Where, for the first time, *institutions had become so large and centralized that they were no longer able to monitor and therefore control each one of their individual members*.
And the solution that he devised was an architectural design - originally intended to be implemented in prisons - that he called the panopticon.”

–Glenn Greenwald, “Why Privacy Matters” @ TED 2014
https://www.ted.com/talks/glenn_greenwald_why_privacy_matters



“The primary attribute of which was the construction of an enormous tower in the center of the institution where whoever controlled the institution could, at any moment, watch any of the inmates, although they couldn’t watch all of them at all times.
And crucial to this design was that *the inmates could not see into the panopticon*, into the tower, and so they never knew if they were being watched.”

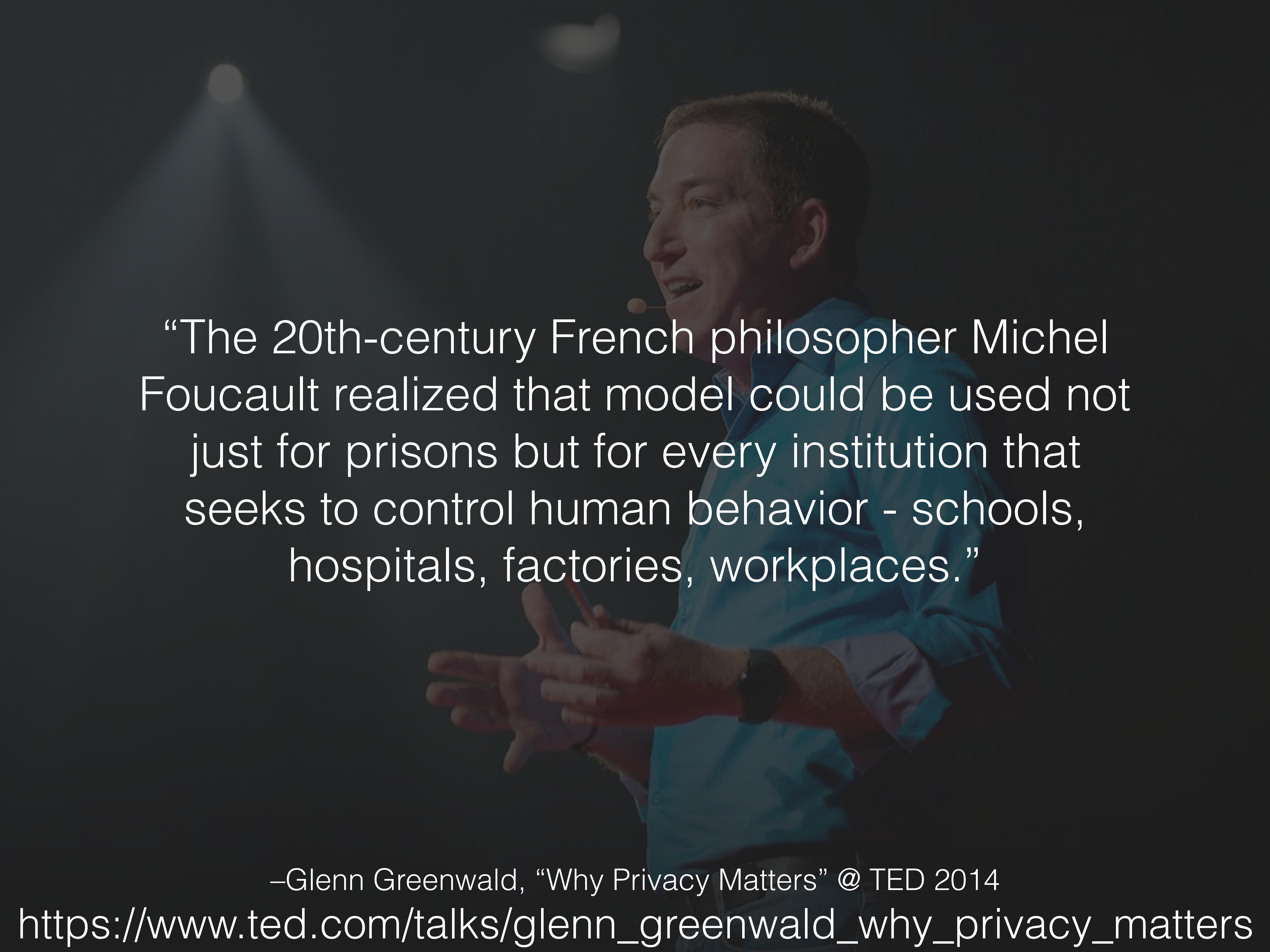
–Glenn Greenwald, “Why Privacy Matters” @ TED 2014
https://www.ted.com/talks/glenn_greenwald_why_privacy_matters



"And what made him so excited about this discovery was that would mean the prisoners would have to *assume that they were being watched at any given moment*, which would be the ultimate enforcer for obedience and compliance."

–Glenn Greenwald, "Why Privacy Matters" @ TED 2014

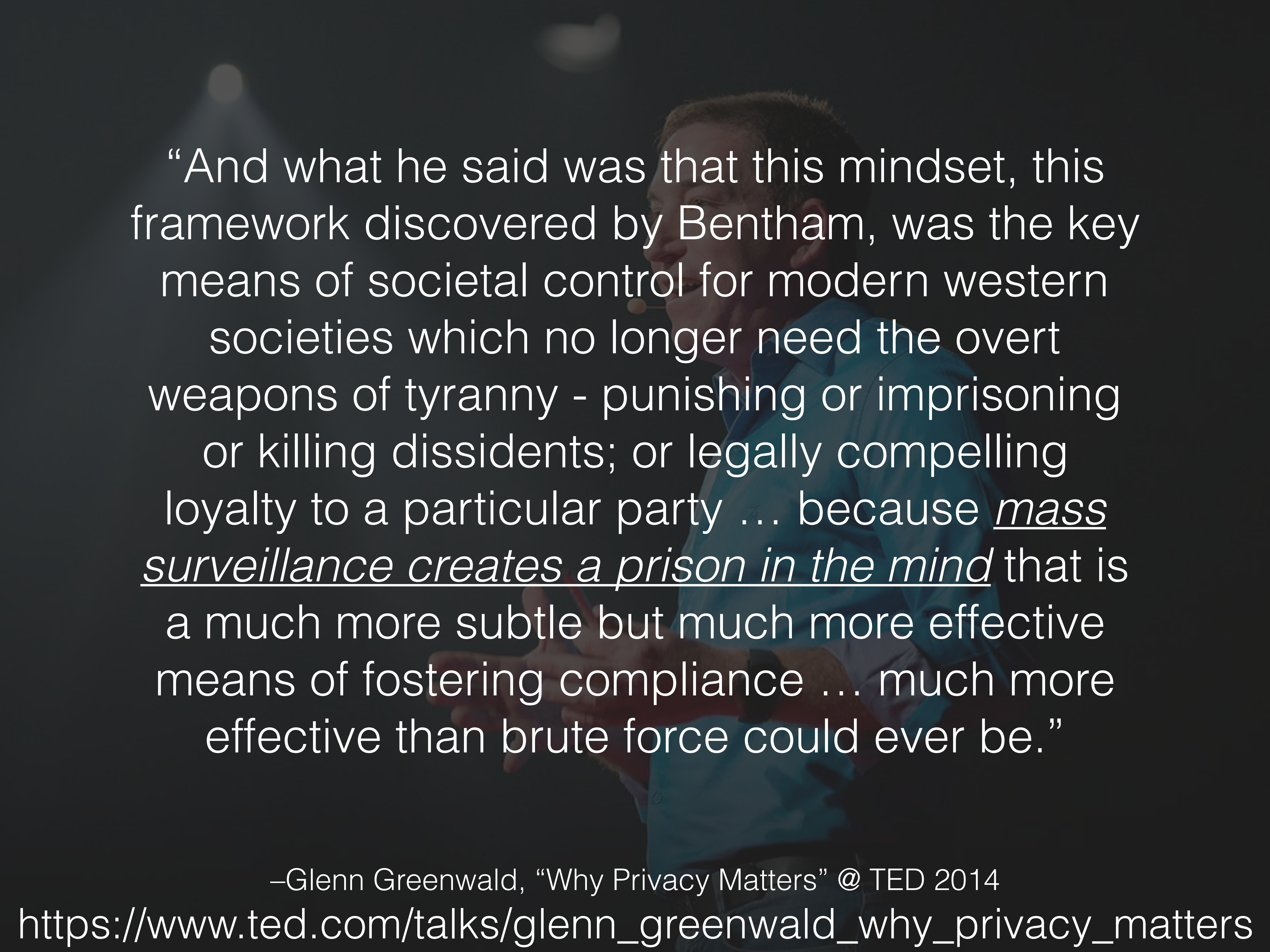
https://www.ted.com/talks/glenn_greenwald_why_privacy_matters



> “The 20th-century French philosopher Michel Foucault realized that model could be used not just for prisons but for every institution that seeks to control human behavior - schools, hospitals, factories, workplaces.”

–Glenn Greenwald, “Why Privacy Matters” @ TED 2014

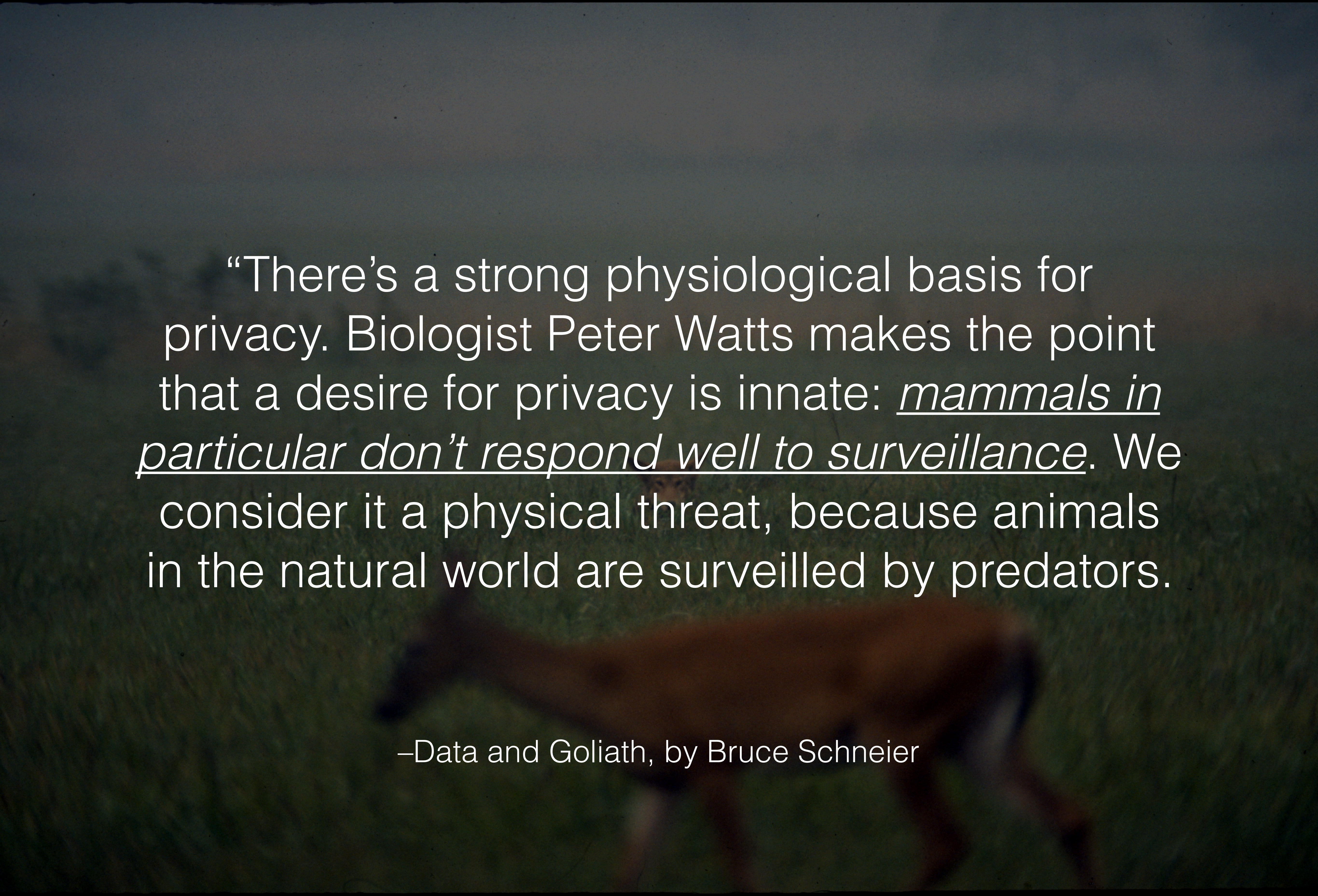
https://www.ted.com/talks/glenn_greenwald_why_privacy_matters



“And what he said was that this mindset, this framework discovered by Bentham, was the key means of societal control for modern western societies which no longer need the overt weapons of tyranny - punishing or imprisoning or killing dissidents; or legally compelling loyalty to a particular party … because *mass surveillance creates a prison in the mind* that is a much more subtle but much more effective means of fostering compliance … much more effective than brute force could ever be.”

–Glenn Greenwald, “Why Privacy Matters” @ TED 2014

https://www.ted.com/talks/glenn_greenwald_why_privacy_matters



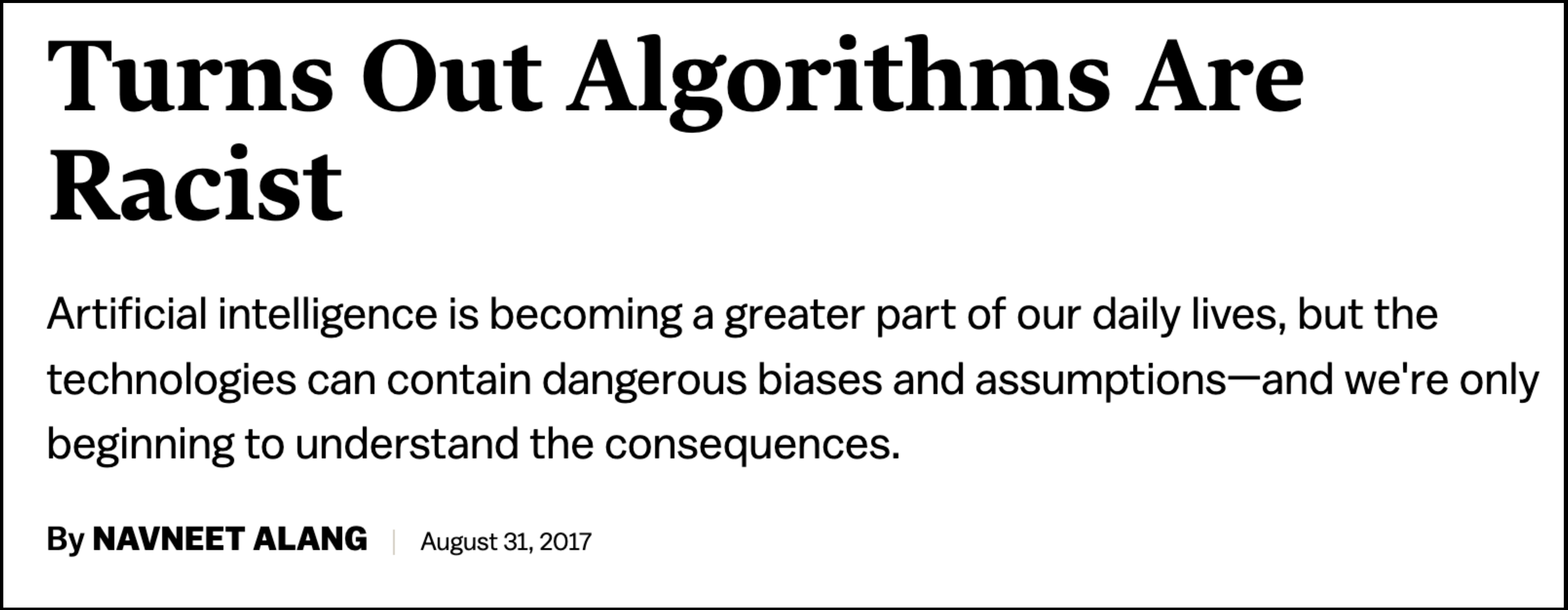
“There’s a strong physiological basis for privacy. Biologist Peter Watts makes the point that a desire for privacy is innate: *mammals in particular don’t respond well to surveillance*. We consider it a physical threat, because animals in the natural world are surveilled by predators.

–Data and Goliath, by Bruce Schneier

> “Surveillance makes us feel like prey, just as it makes surveyors act like predators.”
>
> –Data and Goliath, by Bruce Schneier

Surveillance is not just about free speech and privacy

Behavior Profiling can be racist



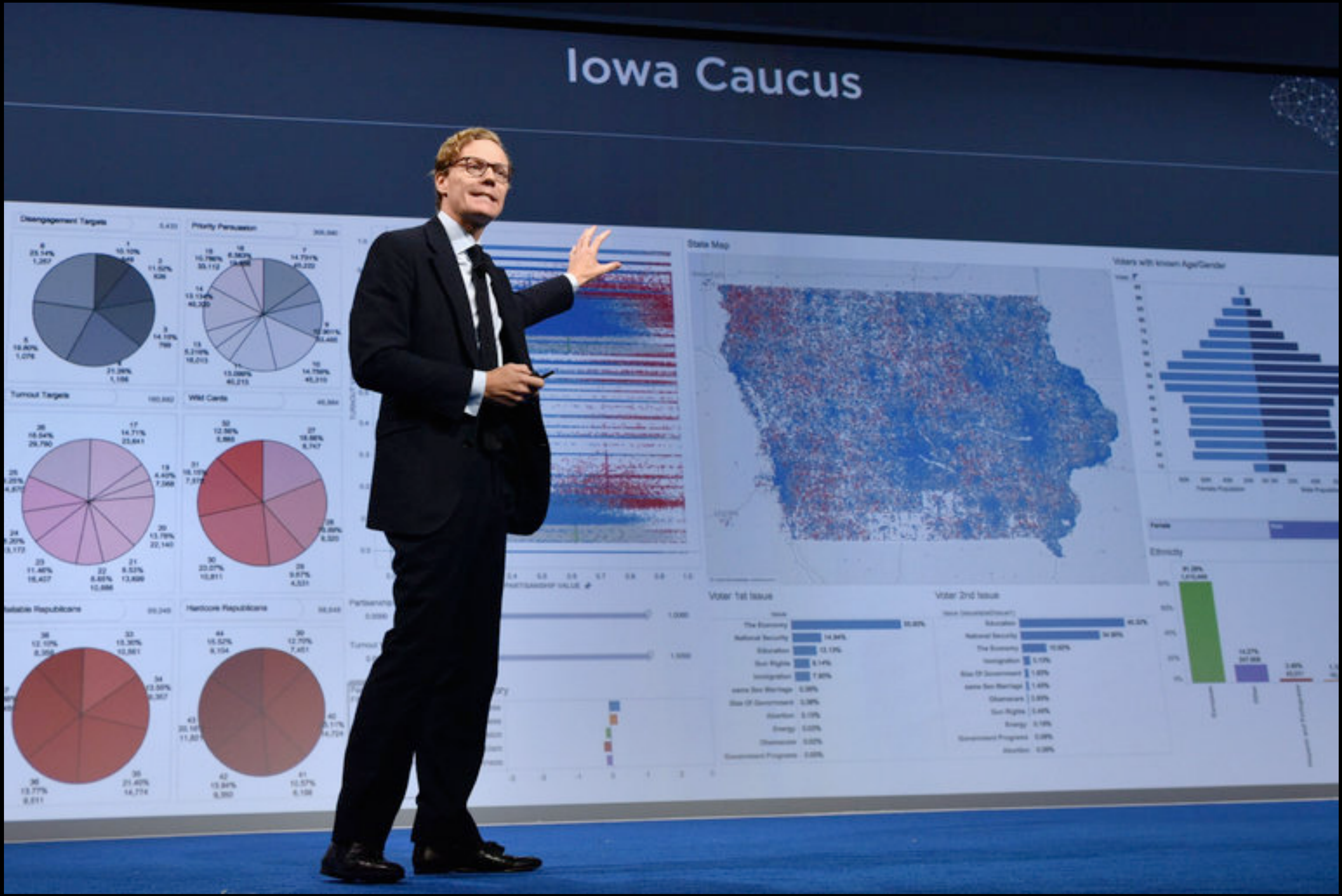
Turns Out Algorithms Are Racist

Artificial intelligence is becoming a greater part of our daily lives, but the technologies can contain dangerous biases and assumptions—and we're only beginning to understand the consequences.

By **NAVNEET ALANG** | August 31, 2017

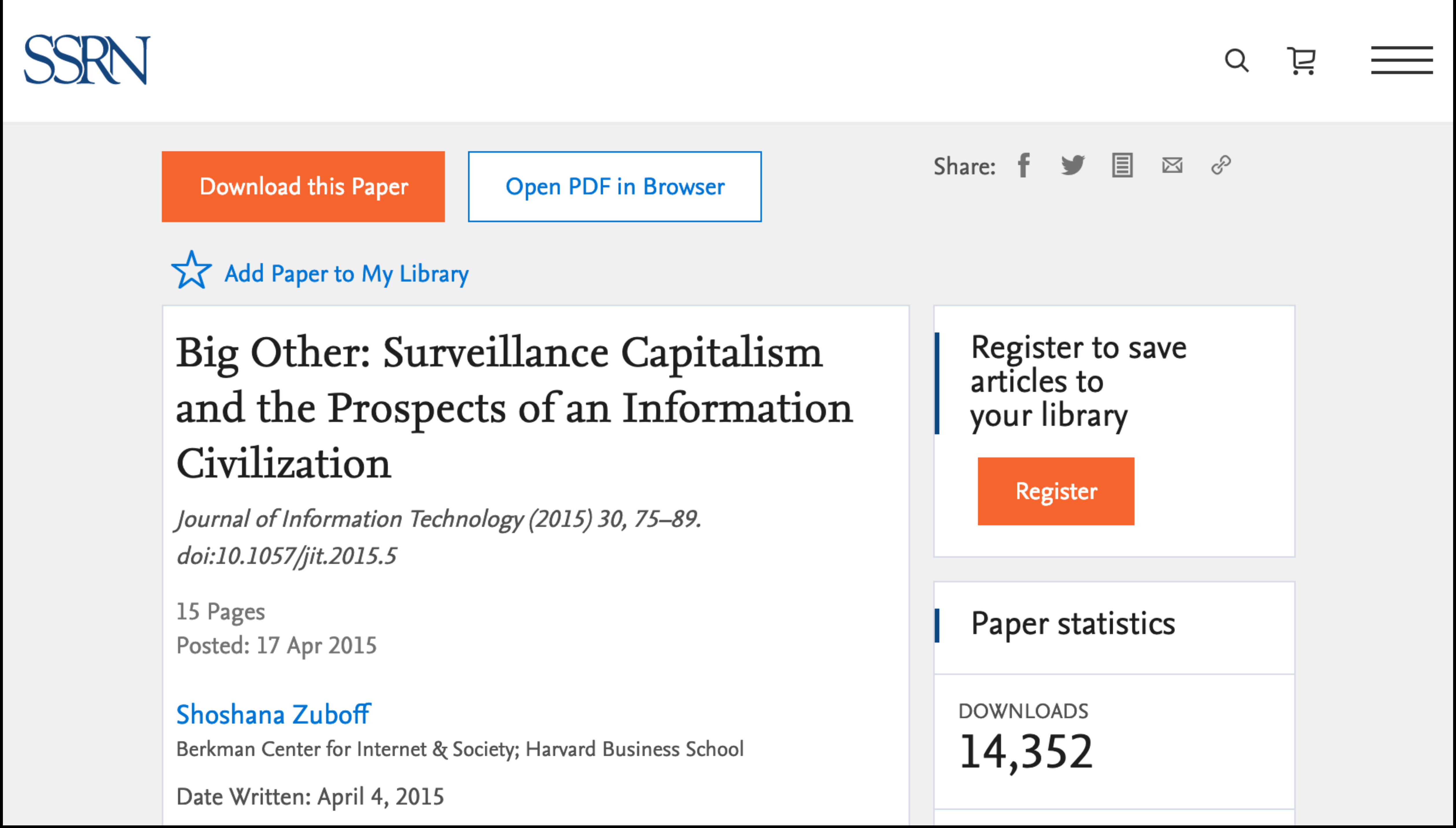
https://newrepublic.com/article/144644/turns-algorithms-racist

Behavior profiling, or Behavior Manipulation?



https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win

“Surveillance Capitalism” can make corporations more powerful than governments



Big Other: Surveillance Capitalism and the Prospects of an Information Civilization

Journal of Information Technology (2015) 30, 75–89. doi:10.1057/jit.2015.5

15 Pages
Posted: 17 Apr 2015

Shoshana Zuboff
Berkman Center for Internet & Society; Harvard Business School

Date Written: April 4, 2015

Register to save articles to your library

Paper statistics

DOWNLOADS
14,352

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754

I’m not a perfectionist

If Google, the NSA, or the FBI want to watch me specifically, they will, and I can’t stop them

I’m a realist who doesn’t
want to be sucked up
into the digital dragnet

What’s next?

What’s next?

- DNS-over-HTTPS / Trusted Recursive Resolver
- Do Not Track v2 ?
    - Policy by Electronic Frontier Foundation
- Single Trust & Same Origin Policy v2 ?
    - proposed by Apple to WebAppSec Working Group

Questions?

- Clear cookies after every browsing session
- No 3rd-party cookies
  - Except from visited sites (Like Safari ITP)
- Strip paths from `Referers` to 3rd parties
- Tracking Protection (Firefox, Safari, Tor)
- First-Party Isolation (Firefox, Tor)
- Resist Fingerprinting (Firefox, Tor)

- DNS-over-HTTPS
- Do Not Track v2
- Same Origin Policy v2 & Single Trust