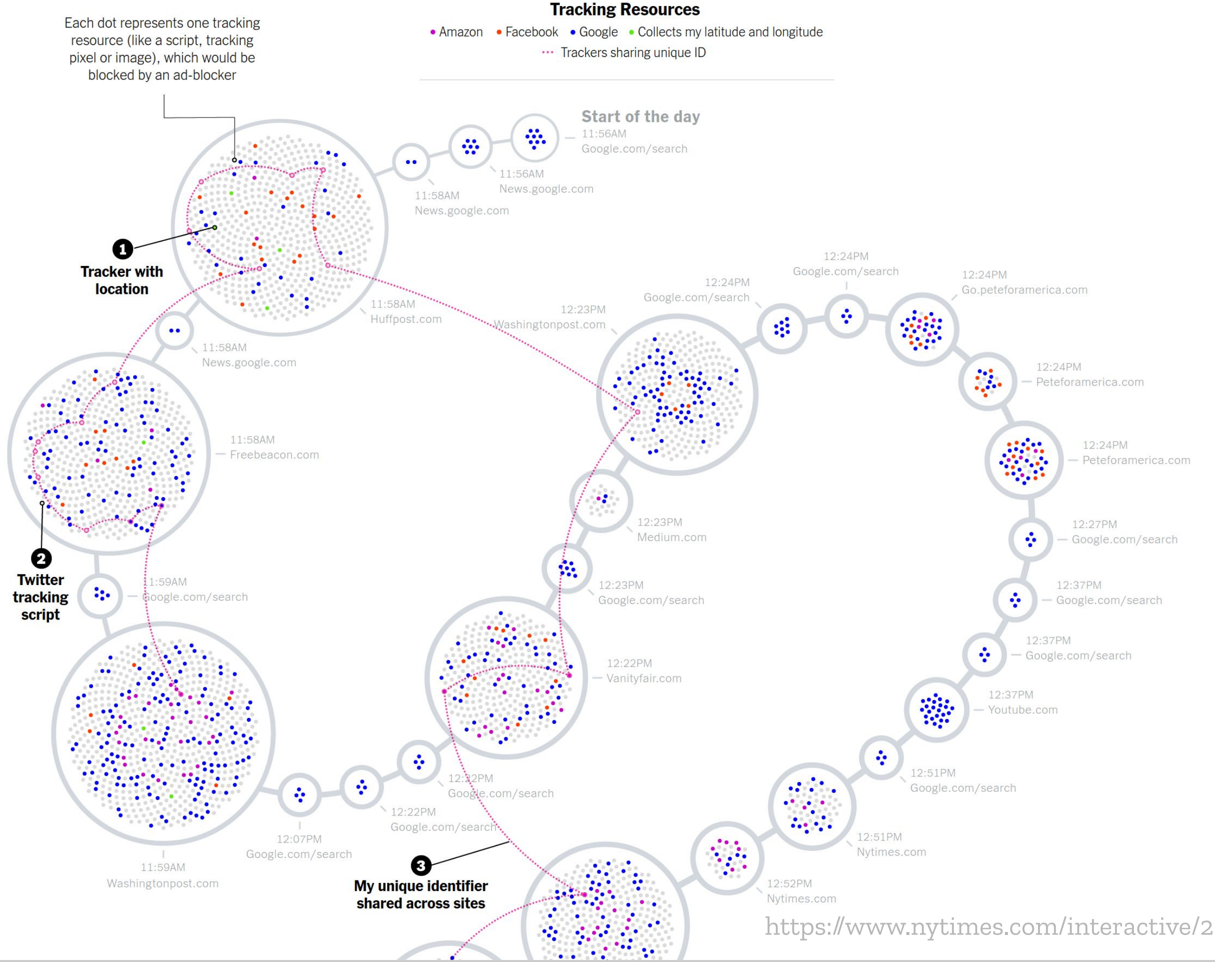
Challenges in building a private web

(without burning it all down)

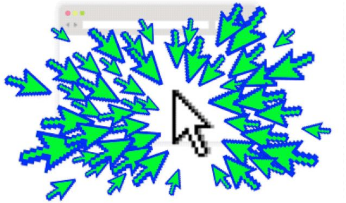
Steven Englehardt

Privacy Engineer

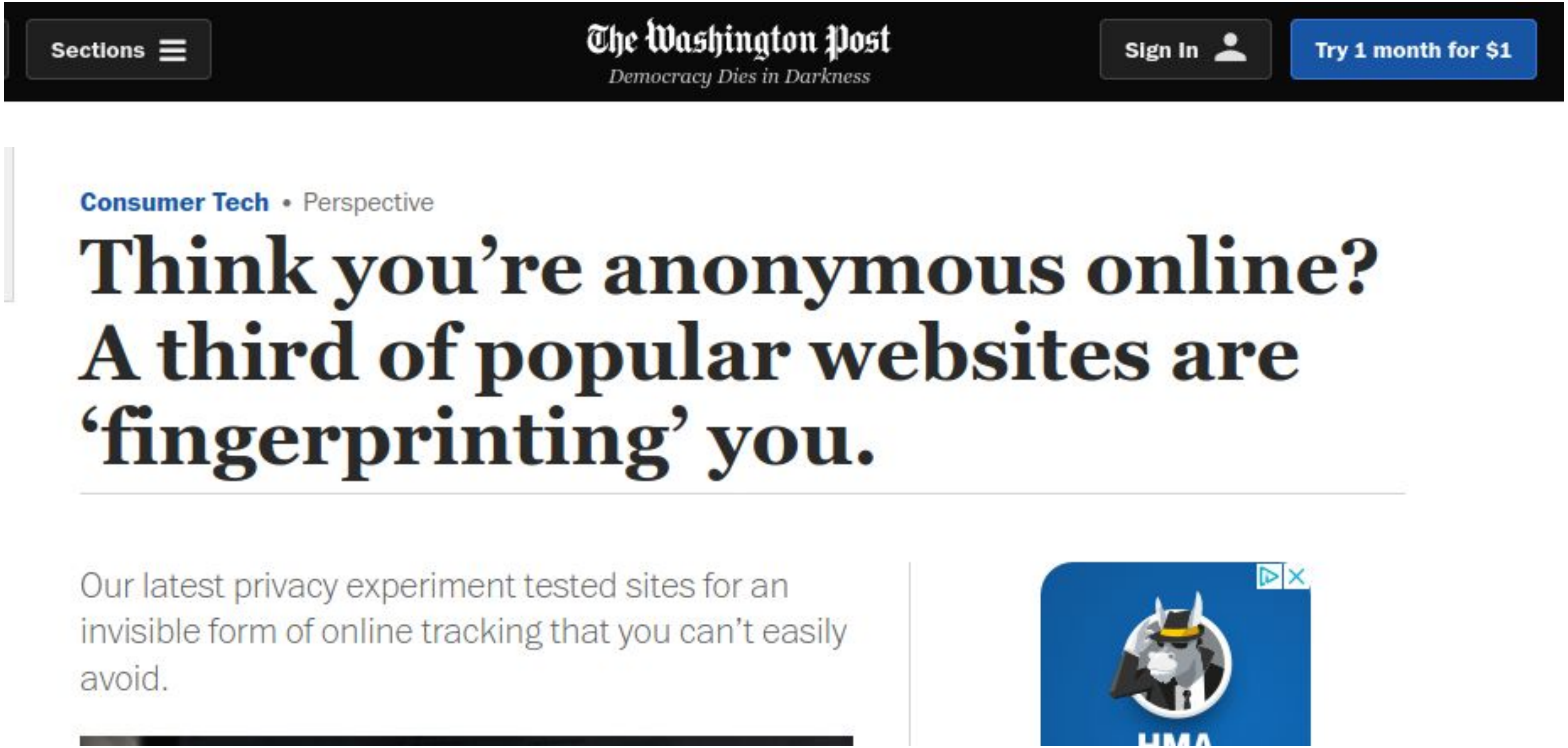


I Visited 47 Sites. Hundreds of Trackers Followed Me.

By Farhad Manjoo
Graphics by Nadieh Bremer



https://www.nytimes.com/interactive/2019/08/23/opinion/data-internet-privacy-tracking.html



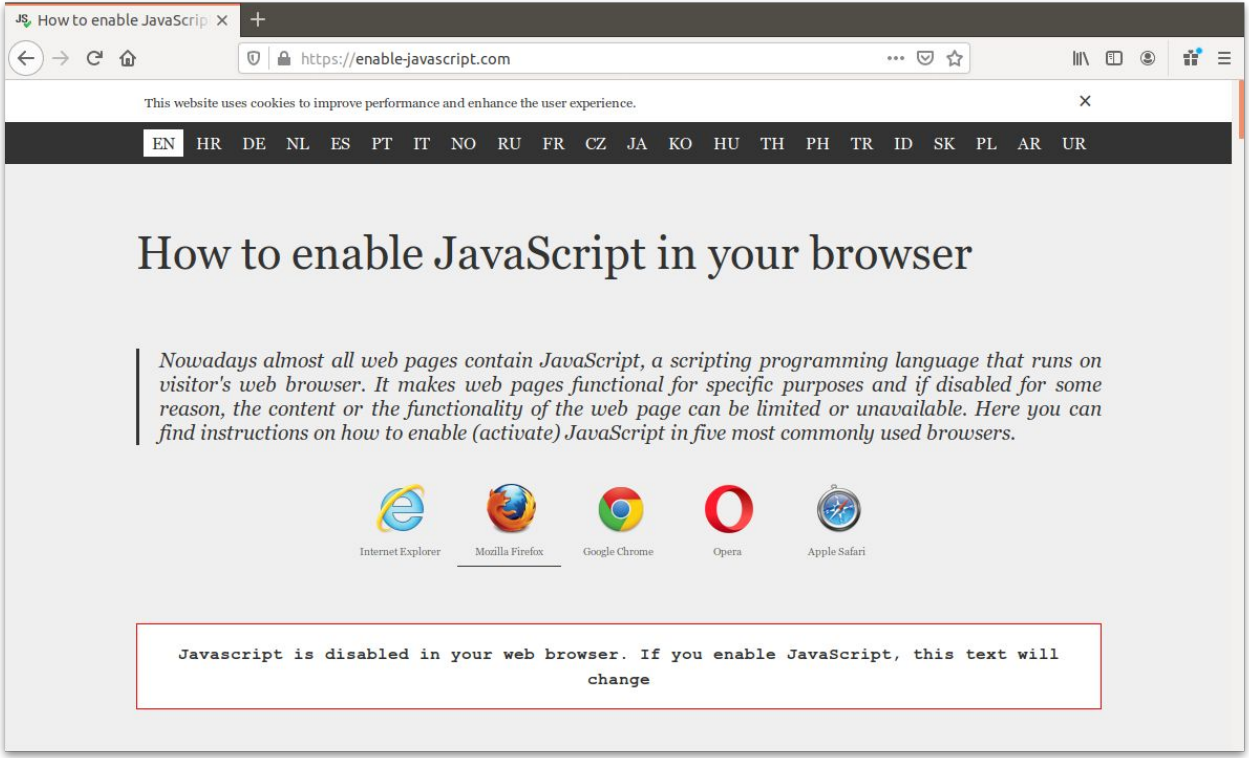
Consumer Tech • Perspective

Think you're anonymous online? A third of popular websites are 'fingerprinting' you.

Our latest privacy experiment tested sites for an invisible form of online tracking that you can't easily avoid.

https://www.washingtonpost.com/technology/2019/10/31/think-youre-anonymous-online-third-popular-websites-are-fingerprinting-you/

Let's just block it all! Who needs Javascript or cookies?



How to enable JavaScrip
https://enable-javascript.com

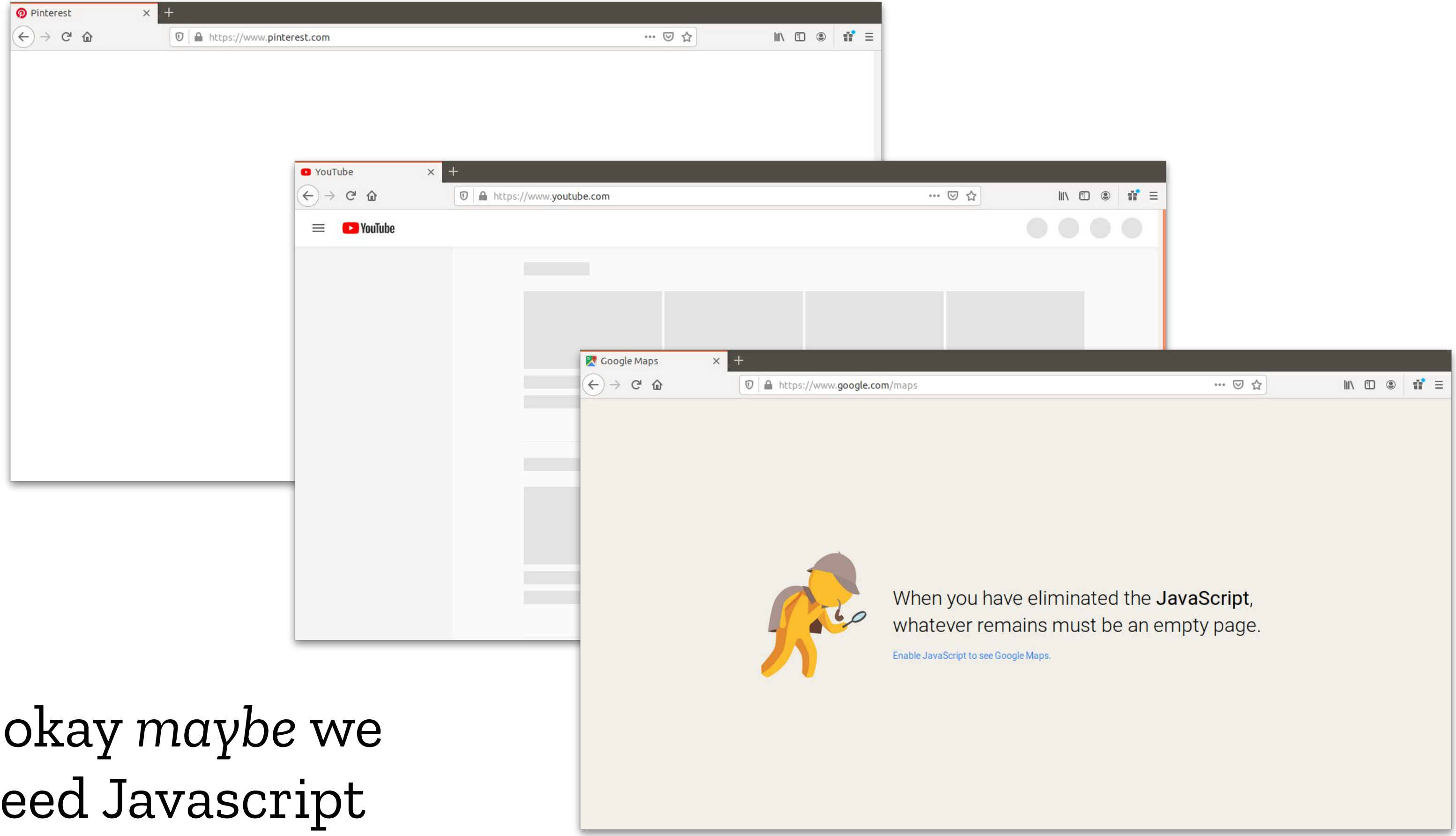
This website uses cookies to improve performance and enhance the user experience.

EN HR DE NL ES PT IT NO RU FR CZ JA KO HU TH PH TR ID SK PL AR UR

How to enable JavaScript in your browser

> *Nowadays almost all web pages contain JavaScript, a scripting programming language that runs on visitor's web browser. It makes web pages functional for specific purposes and if disabled for some reason, the content or the functionality of the web page can be limited or unavailable. Here you can find instructions on how to enable (activate) JavaScript in five most commonly used browsers.*

Javascript is disabled in your web browser. If you enable JavaScript, this text will change



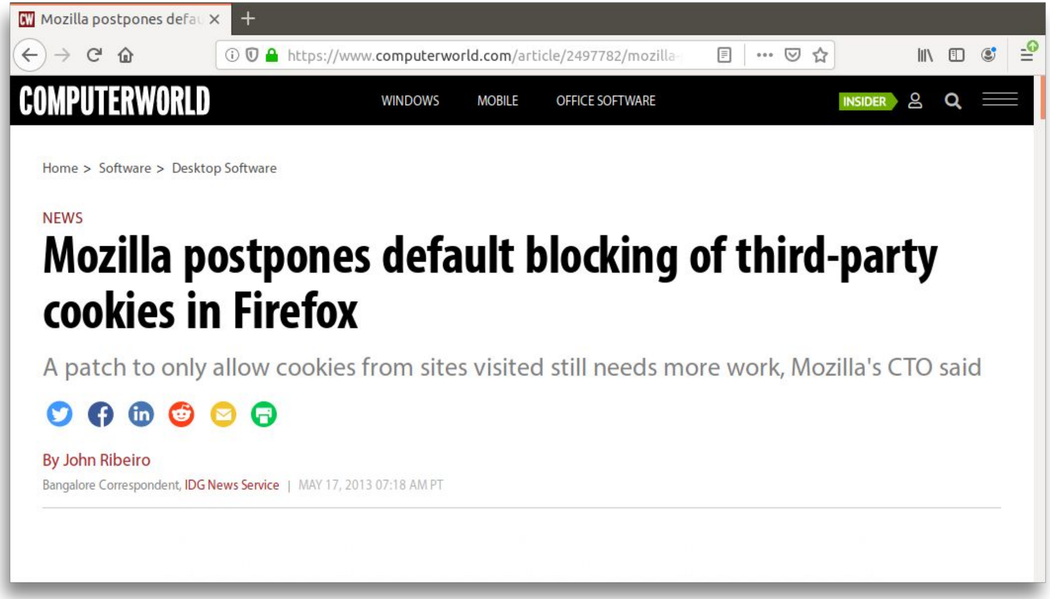
When you have eliminated the **JavaScript**, whatever remains must be an empty page.

Enable JavaScript to see Google Maps.

...okay *maybe* we need Javascript

Can we at least block all third-party cookies?

We've tried that back in 2013...



Home > Software > Desktop Software

NEWS

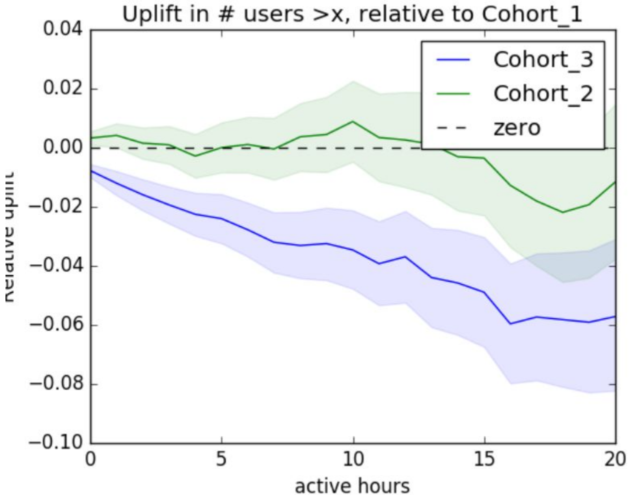
Mozilla postpones default blocking of third-party cookies in Firefox

A patch to only allow cookies from sites visited still needs more work, Mozilla's CTO said

By John Ribeiro

Bangalore Correspondent, IDG News Service | MAY 17, 2013 07:18 AM PT

Can we at least block all third-party cookies?



Cohort_3: Block all third-party cookies
Cohort_2: Block cookies from trackers
Cohort_1: Control; No blocking

Compared to no blocking, users who had all third-party cookies blocked (over a 1 - 2 week study period):

- ~1% fewer active users overall
- 2 - 5% fewer users active over 10 hours

The drop was so significant, we ended this part of the study immediately.

https://mozilla.report/post/projects/cookie_restrictions.kp/

The core problem: one identifier, many uses

id=LgzcCiQvIbXtXjtkWrOZ

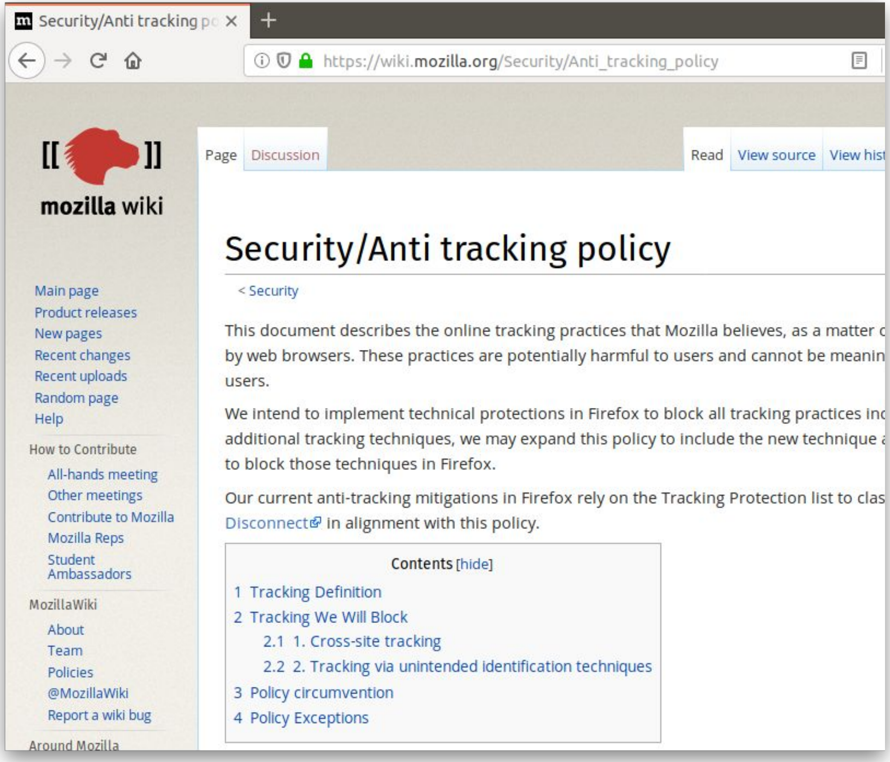
- Cross-site tracking
- Ad performance tracking
- Federated login
- First-party login
- Fraud detection
- Captcha / device reputation
- Analytics
- … and many more

Our approach to anti-tracking…

1. No configuration necessary; **private by default**.
2. **Block the trackers**, not necessarily the tracking capability.
3. Don't break experiences **users care about**.

"[T]racking practices that Mozilla believes, as a matter of policy, **should be blocked** by default **by web browsers.**"

1. **Cross-site tracking:**
   a. Cookie-based
   b. URL parameter-based
2. **Unintended identification techniques:**
   a. Browser fingerprinting
   b. Supercookies



Security/Anti tracking policy

< Security

This document describes the online tracking practices that Mozilla believes, as a matter c
by web browsers. These practices are potentially harmful to users and cannot be meanin
users.

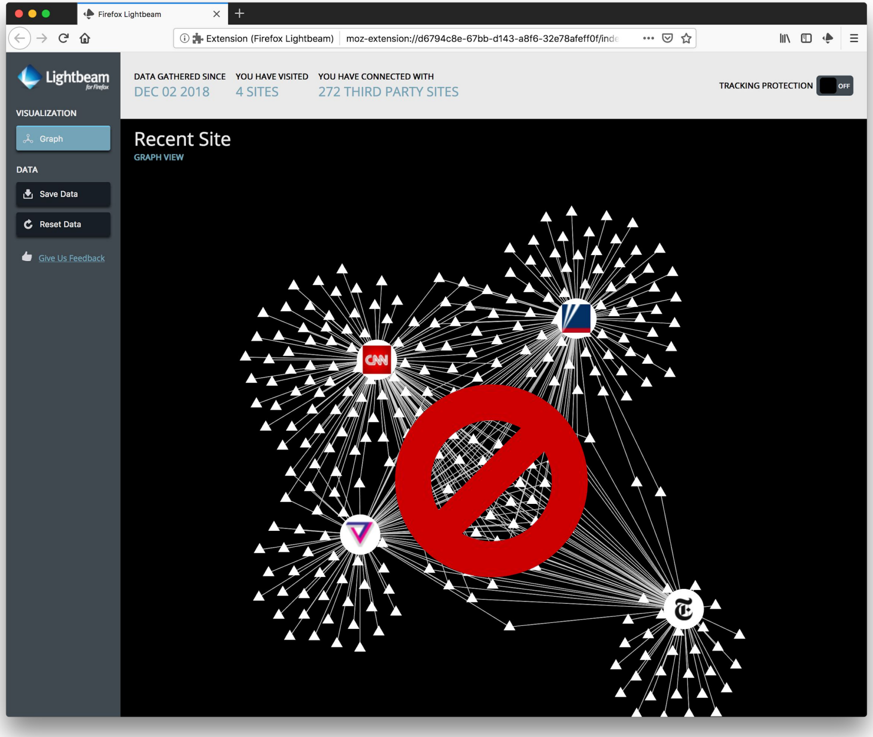
We intend to implement technical protections in Firefox to block all tracking practices inc
additional tracking techniques, we may expand this policy to include the new technique a
to block those techniques in Firefox.

Our current anti-tracking mitigations in Firefox rely on the Tracking Protection list to clas
Disconnect in alignment with this policy.

Contents [hide]

1 Tracking Definition
2 Tracking We Will Block
2.1 1. Cross-site tracking
2.2 2. Tracking via unintended identification techniques
3 Policy circumvention
4 Policy Exceptions

Our first step: Block only **tracking** cookies



Extension (Firefox Lightbeam) moz-extension://d6794c8e-67bb-d143-a8f6-32e78afeff0f/inde

DATA GATHERED SINCE DEC 02 2018

YOU HAVE VISITED 4 SITES

YOU HAVE CONNECTED WITH 272 THIRD PARTY SITES

TRACKING PROTECTION OFF

Recent Site

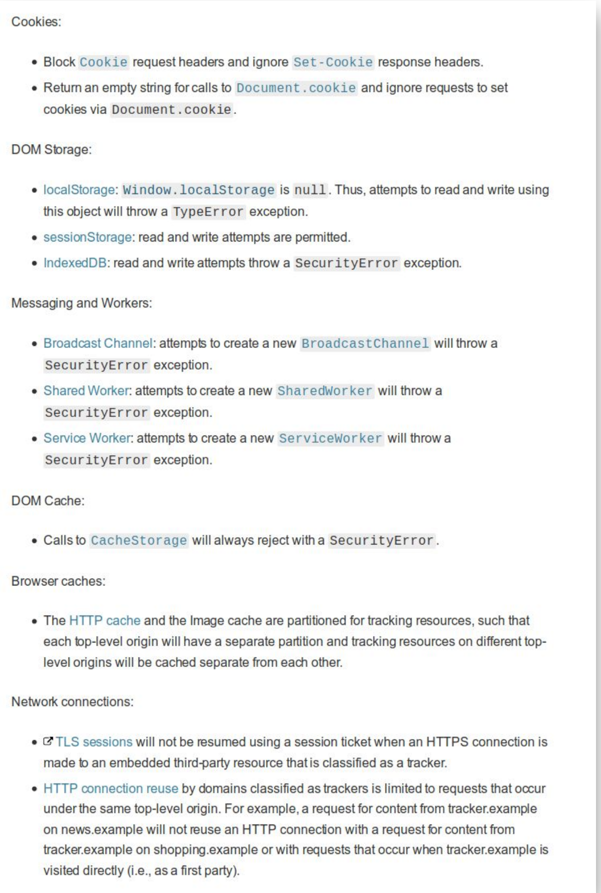
GRAPH VIEW

Trackers are identified by Disconnect, based on a review of privacy policies.

It's more than just cookies...

We block all of this →

for all domains on the Disconnect Tracking Protection list



Cookies:

- Block `Cookie` request headers and ignore `Set-Cookie` response headers.
- Return an empty string for calls to `Document.cookie` and ignore requests to set cookies via `Document.cookie`.

DOM Storage:

- localStorage: `Window.localStorage` is `null`. Thus, attempts to read and write using this object will throw a `TypeError` exception.
- sessionStorage: read and write attempts are permitted.
- IndexedDB: read and write attempts throw a `SecurityError` exception.

Messaging and Workers:

- Broadcast Channel: attempts to create a new `BroadcastChannel` will throw a `SecurityError` exception.
- Shared Worker: attempts to create a new `SharedWorker` will throw a `SecurityError` exception.
- Service Worker: attempts to create a new `ServiceWorker` will throw a `SecurityError` exception.

DOM Cache:

- Calls to `CacheStorage` will always reject with a `SecurityError`.

Browser caches:

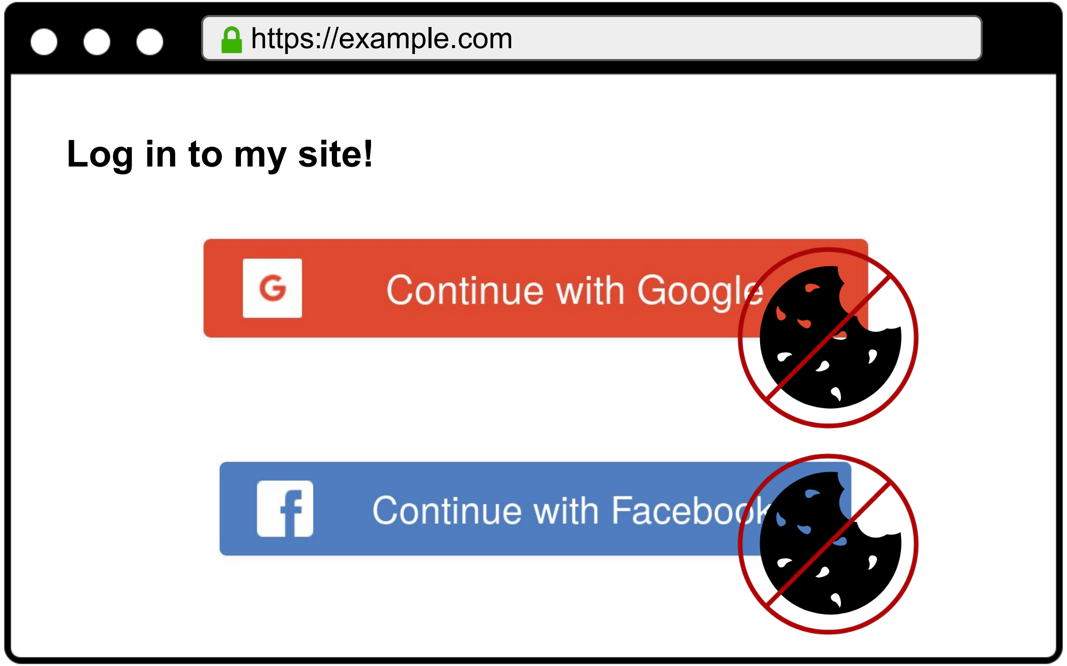
- The HTTP cache and the Image cache are partitioned for tracking resources, such that each top-level origin will have a separate partition and tracking resources on different top-level origins will be cached separate from each other.

Network connections:

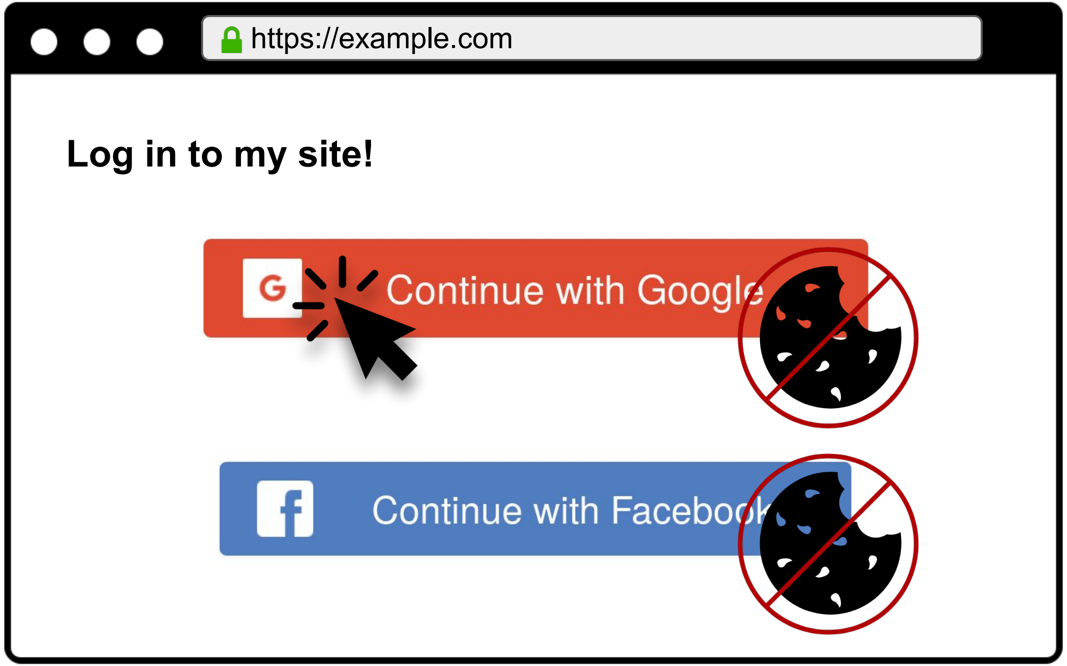
- TLS sessions will not be resumed using a session ticket when an HTTPS connection is made to an embedded third-party resource that is classified as a tracker.
- HTTP connection reuse by domains classified as trackers is limited to requests that occur under the same top-level origin. For example, a request for content from tracker.example on news.example will not reuse an HTTP connection with a request for content from tracker.example on shopping.example or with requests that occur when tracker.example is visited directly (i.e., as a first party).

https://developer.mozilla.org/en-US/docs/Mozilla/Firefox/Privacy/Storage_access_policy

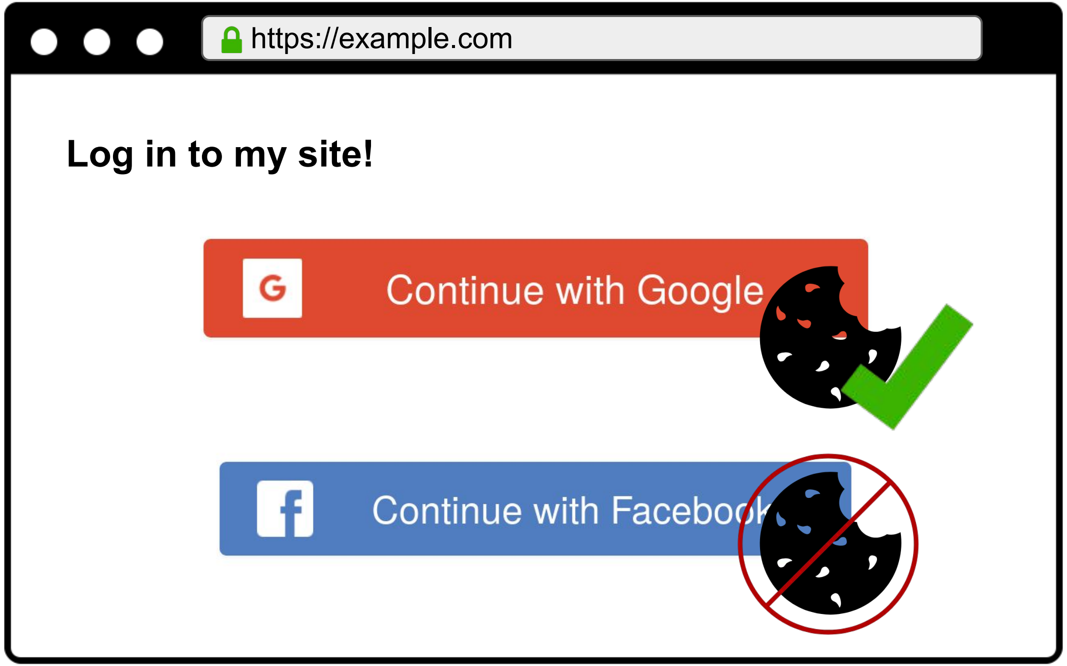
Some tracking is dual-use



Key insight: users interact with these services!



Cookies permitted after interaction, but **only on** example.com

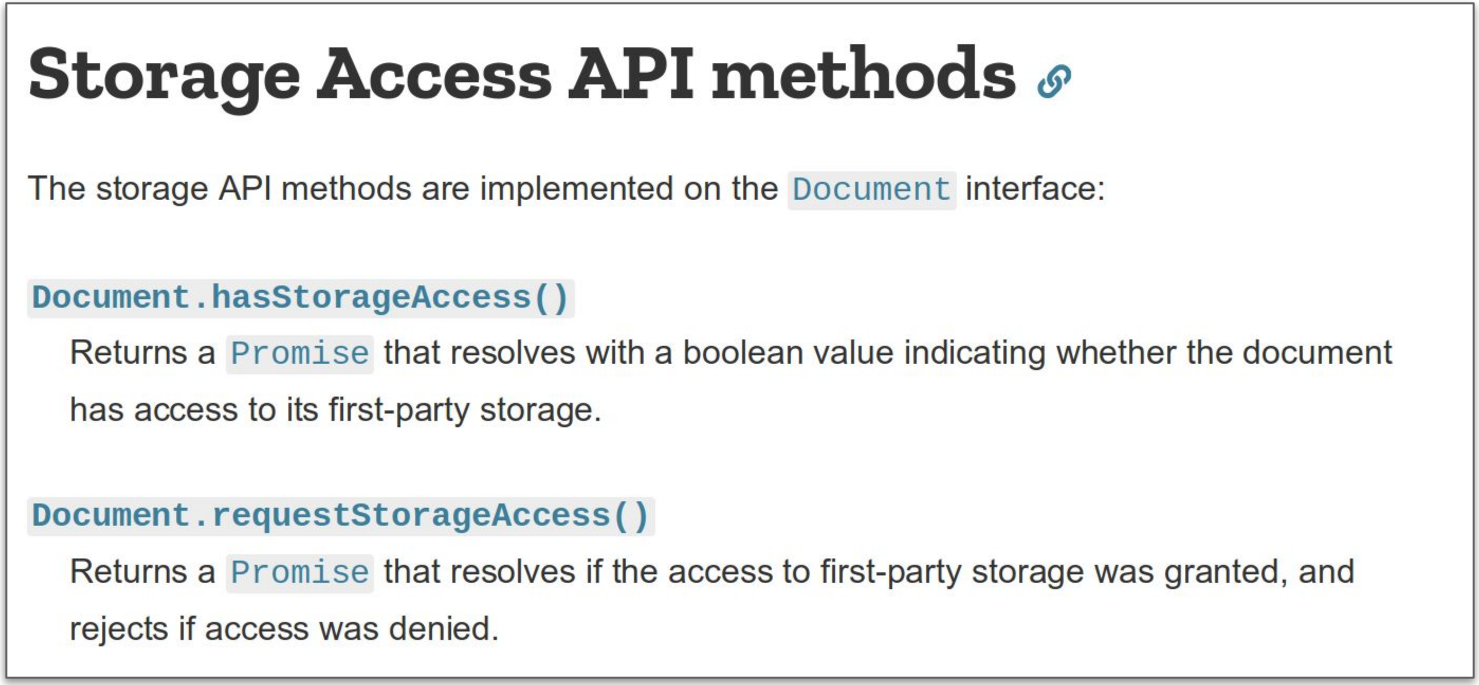


https://example.com

Log in to my site!

https://developer.mozilla.org/en-US/docs/Mozilla/Firefox/Privacy/Storage_access_policy

Programmatic cookie access: the Storage Access API



Storage Access API methods

The storage API methods are implemented on the `Document` interface:

`Document.hasStorageAccess()`

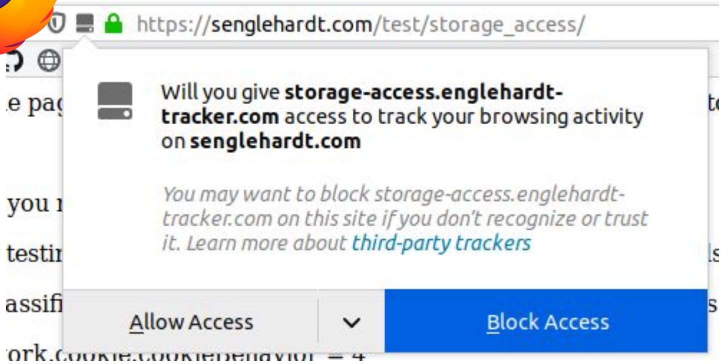
Returns a `Promise` that resolves with a boolean value indicating whether the document has access to its first-party storage.

`Document.requestStorageAccess()`

Returns a `Promise` that resolves if the access to first-party storage was granted, and rejects if access was denied.

https://developer.mozilla.org/en-US/docs/Web/API/Storage_Access_API

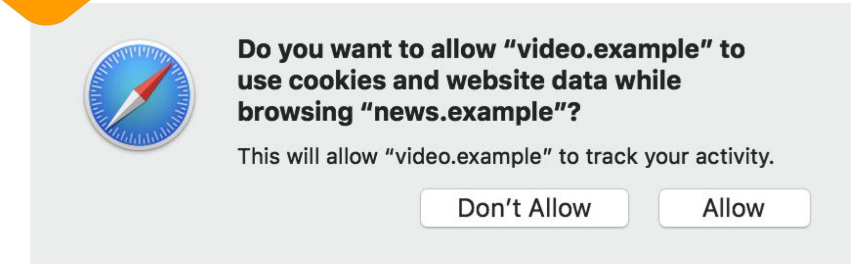
Programmatic cookie access: the Storage Access API



https://senglehardt.com/test/storage_access/

Will you give **storage-access.englehardt-tracker.com** access to track your browsing activity on **senglehardt.com**

You may want to block storage-access.englehardt-tracker.com on this site if you don't recognize or trust it. Learn more about third-party trackers



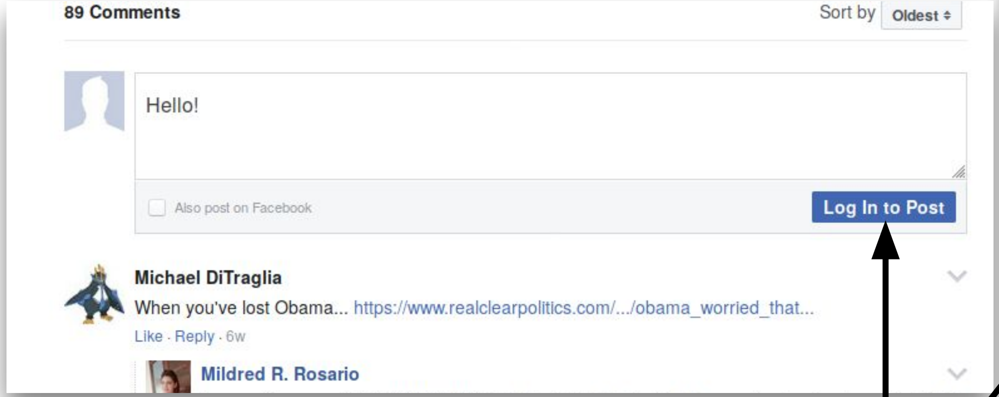
Do you want to allow "video.example" to use cookies and website data while browsing "news.example"?

This will allow "video.example" to track your activity.

Notable differences in the prompting heuristics and scope of granted access:

- https://developer.mozilla.org/en-US/docs/Web/API/Document/requestStorageAccess#Conditions_for_granting_storage_access
- https://developer.mozilla.org/en-US/docs/Web/API/Storage_Access_API#Safari_implementation_differences

We're seeing adoption of the Storage Access API



89 Comments

Sort by Oldest ÷

Hello!

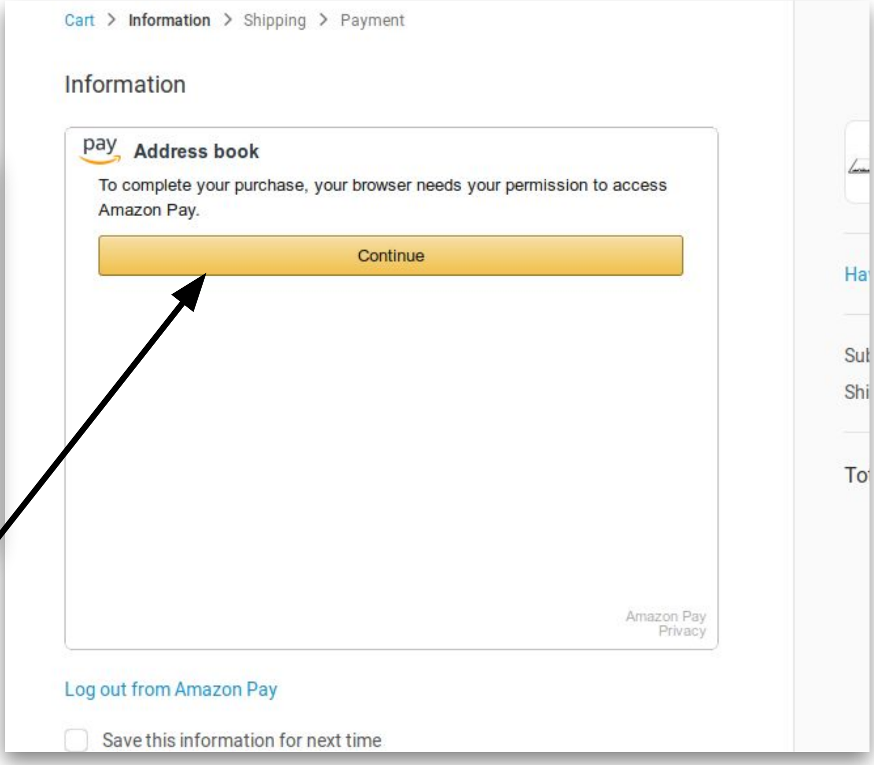
□ Also post on Facebook

Michael DiTraglia

When you've lost Obama... https://www.realclearpolitics.com/.../obama_worried_that...

Like · Reply · 6w

Mildred R. Rosario



Information

pay **Address book**

To complete your purchase, your browser needs your permission to access Amazon Pay.

Amazon Pay
Privacy

Log out from Amazon Pay

□ Save this information for next time

calls Document.requestStorageAccess()

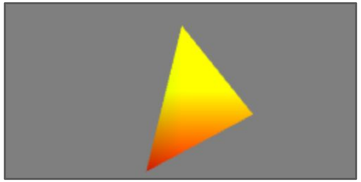
The next step: browser fingerprinting

Locale

Screen Size

User Agent

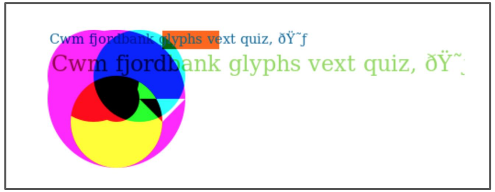
WebGL



Font probing

```
Times New Roman, Arial,
Open Sans, Courier New,
Georgia, Comic Sans, ...
```

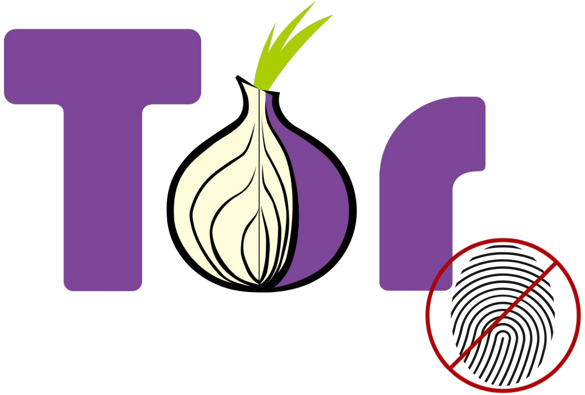
HTML Canvas


Cwm fjordbank glyphs vext quiz, ðŸ˜ƒ
Cwm fjordbank glyphs vext quiz, ðŸ˜

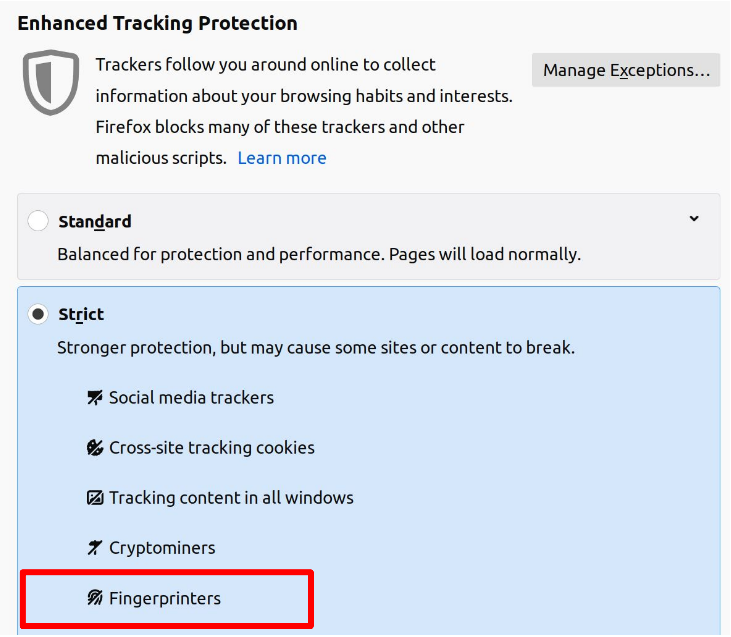
Fingerprinting use is still growing...

2016	2019
~1.6% of the Alexa top 1M	~3.8% of the Alexa top 1M
Englehardt & Narayanan; Online Tracking (CCS2016)	*Unpublished OpenWPM measurements from Feb 2019*

Two general approaches to anti-fingerprinting



Tor Browser's anti-fingerprinting in Firefox behind `privacy.resistFingerprinting`



Enhanced Tracking Protection

Trackers follow you around online to collect information about your browsing habits and interests. Firefox blocks many of these trackers and other malicious scripts. Learn more

○ **Standard**

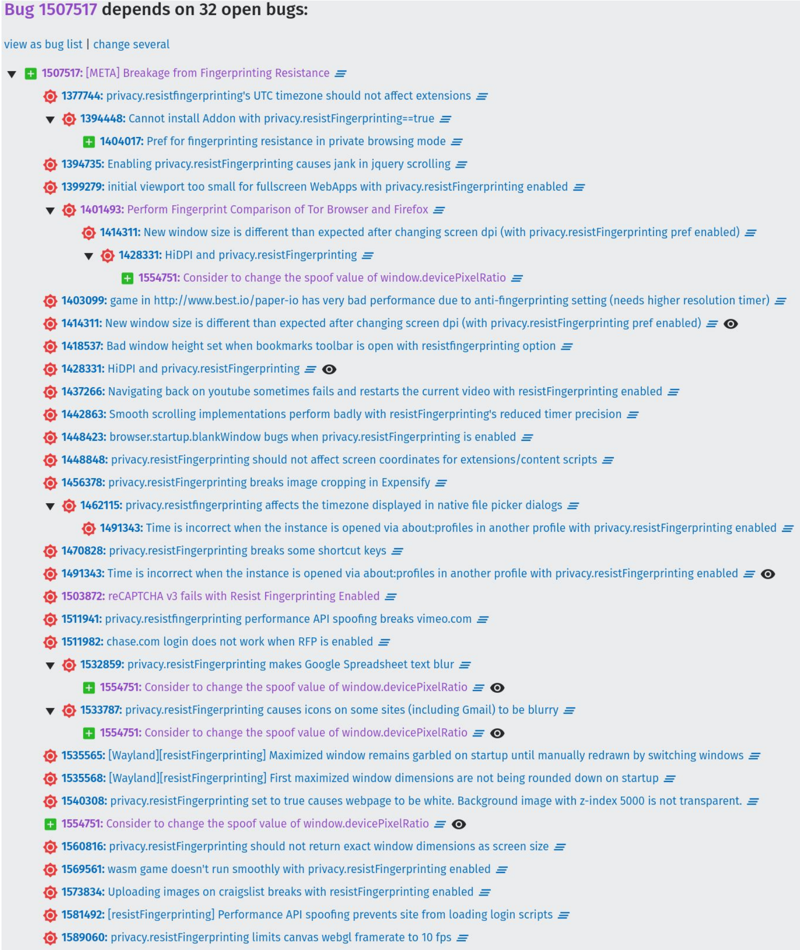
Balanced for protection and performance. Pages will load normally.

● **Strict**

Stronger protection, but may cause some sites or content to break.

- Social media trackers
- Cross-site tracking cookies
- Tracking content in all windows
- Cryptominers
- Fingerprinters

Firefox 70



Bug 1507517 depends on 32 open bugs:

view as bug list | change several

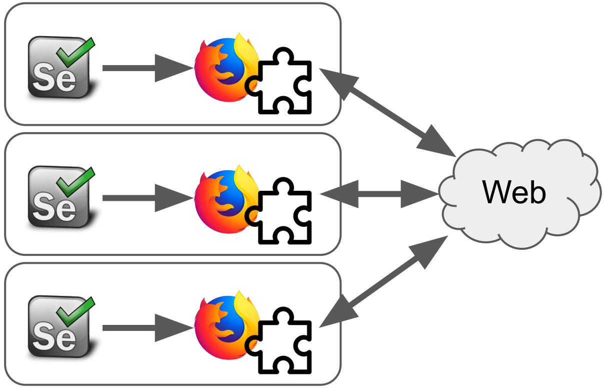
- ▼ **1507517:** [META] Breakage from Fingerprinting Resistance
  - **1377744:** privacy.resistfingerprinting's UTC timezone should not affect extensions
  - ▼ **1394448:** Cannot install Addon with privacy.resistFingerprinting==true
    - **1404017:** Pref for fingerprinting resistance in private browsing mode
  - **1394735:** Enabling privacy.resistFingerprinting causes jank in jquery scrolling
  - **1399279:** initial viewport too small for fullscreen WebApps with privacy.resistFingerprinting enabled
  - ▼ **1401493:** Perform Fingerprint Comparison of Tor Browser and Firefox
    - **1414311:** New window size is different than expected after changing screen dpi (with privacy.resistFingerprinting pref enabled)
    - ▼ **1428331:** HiDPI and privacy.resistFingerprinting
      - **1554751:** Consider to change the spoof value of window.devicePixelRatio
  - **1403099:** game in http://www.best.io/paper-io has very bad performance due to anti-fingerprinting setting (needs higher resolution timer)
  - **1414311:** New window size is different than expected after changing screen dpi (with privacy.resistFingerprinting pref enabled)
  - **1418537:** Bad window height set when bookmarks toolbar is open with resistfingerprinting option
  - **1428331:** HiDPI and privacy.resistFingerprinting
  - **1437266:** Navigating back on youtube sometimes fails and restarts the current video with resistFingerprinting enabled
  - **1442863:** Smooth scrolling implementations perform badly with resistFingerprinting's reduced timer precision
  - **1448423:** browser.startup.blankWindow bugs when privacy.resistFingerprinting is enabled
  - **1448848:** privacy.resistFingerprinting should not affect screen coordinates for extensions/content scripts
  - **1456378:** privacy.resistFingerprinting breaks image cropping in Expensify
  - ▼ **1462115:** privacy.resistfingerprinting affects the timezone displayed in native file picker dialogs
    - **1491343:** Time is incorrect when the instance is opened via about:profiles in another profile with privacy.resistFingerprinting enabled
  - **1470828:** privacy.resistFingerprinting breaks some shortcut keys
  - **1491343:** Time is incorrect when the instance is opened via about:profiles in another profile with privacy.resistFingerprinting enabled
  - **1503872:** reCAPTCHA v3 fails with Resist Fingerprinting Enabled
  - **1511941:** privacy.resistfingerprinting performance API spoofing breaks vimeo.com
  - **1511982:** chase.com login does not work when RFP is enabled
  - ▼ **1532859:** privacy.resistFingerprinting makes Google Spreadsheet text blur
    - **1554751:** Consider to change the spoof value of window.devicePixelRatio
  - ▼ **1533787:** privacy.resistFingerprinting causes icons on some sites (including Gmail) to be blurry
    - **1554751:** Consider to change the spoof value of window.devicePixelRatio
  - **1535565:** [Wayland][resistFingerprinting] Maximized window remains garbled on startup until manually redrawn by switching windows
  - **1535568:** [Wayland][resistFingerprinting] First maximized window dimensions are not being rounded down on startup
  - **1540308:** privacy.resistFingerprinting set to true causes webpage to be white. Background image with z-index 5000 is not transparent.
  - **1554751:** Consider to change the spoof value of window.devicePixelRatio
  - **1560816:** privacy.resistFingerprinting should not return exact window dimensions as screen size
  - **1569561:** wasm game doesn't run smoothly with privacy.resistFingerprinting enabled
  - **1573834:** Uploading images on craigslist breaks with resistFingerprinting enabled
  - **1581492:** [resistFingerprinting] Performance API spoofing prevents site from loading login scripts
  - **1589060:** privacy.resistFingerprinting limits canvas webgl framerate to 10 fps

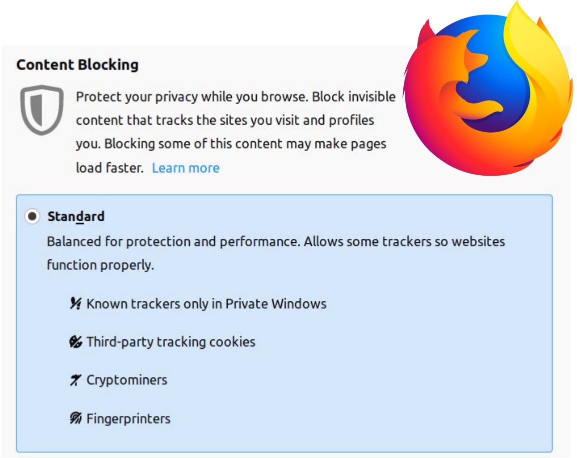
Changing APIs is hard...

- Image scaling problems from changing `devicePixelRatio`
- Image transparency issues
- Framerate and performance problems from timing changes

https://bugzilla.mozilla.org/show_bug.cgi?id=1507517

Our current approach: blocking fingerprinting scripts




Content Blocking

Protect your privacy while you browse. Block invisible content that tracks the sites you visit and profiles you. Blocking some of this content may make pages load faster. Learn more

● **Standard**

Balanced for protection and performance. Allows some trackers so websites function properly.

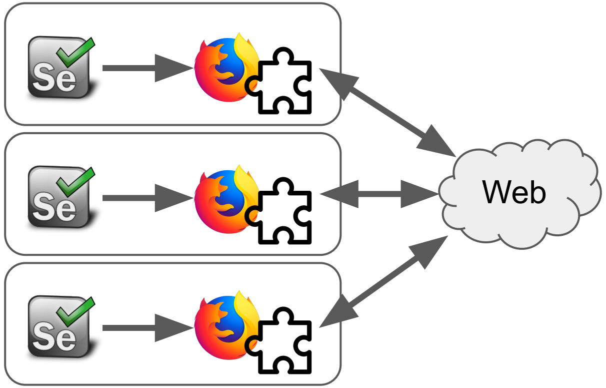
- Known trackers only in Private Windows
- Third-party tracking cookies
- Cryptominers
- Fingerprinters

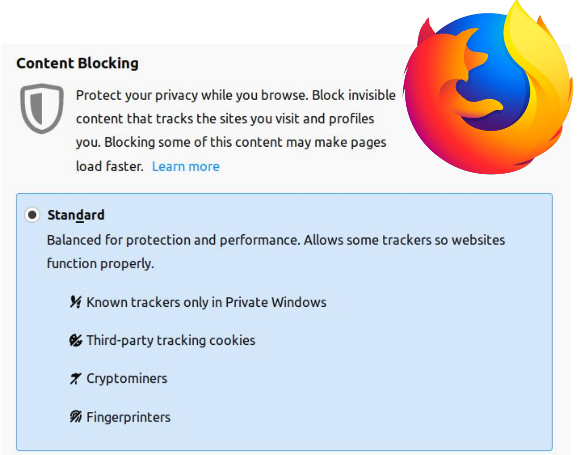
Crawl the web with OpenWPM. Detect fingerprinting scripts.

Share flagged scripts with Disconnect, who does a review to remove false positives.

Domains blocked in Firefox. Eventually by default.

Our current approach: blocking fingerprinting scripts





Content Blocking

Protect your privacy while you browse. Block invisible content that tracks the sites you visit and profiles you. Blocking some of this content may make pages load faster. Learn more

● **Standard**

Balanced for protection and performance. Allows some trackers so websites function properly.

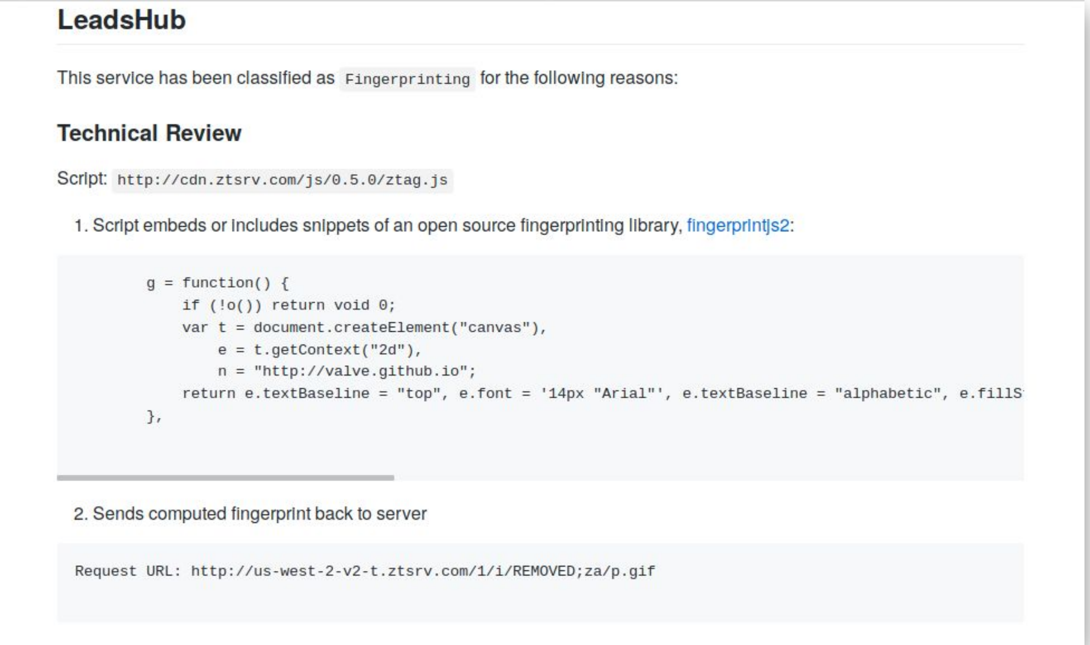
- Known trackers only in Private Windows
- Third-party tracking cookies
- Cryptominers
- Fingerprinters

138 verified fingerprinters

75% of the fingerprinting instances we've detected

Disconnect reviews candidate scripts

An example:



LeadsHub

This service has been classified as `Fingerprinting` for the following reasons:

Technical Review

Script: `http://cdn.ztsrv.com/js/0.5.0/ztag.js`

1. Script embeds or includes snippets of an open source fingerprinting library, fingerprintjs2:

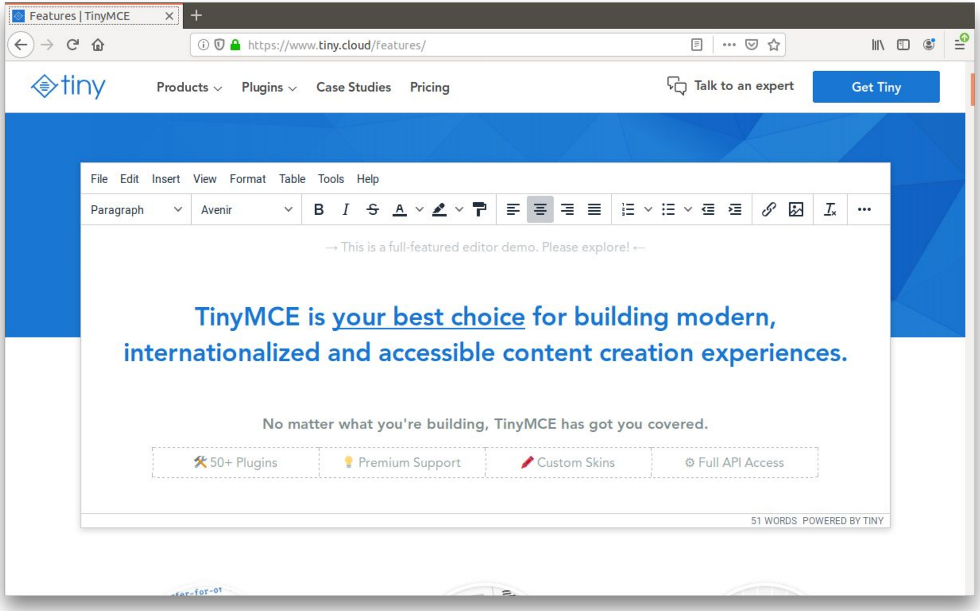
```
        g = function() {
            if (!o()) return void 0;
            var t = document.createElement("canvas"),
                e = t.getContext("2d"),
                n = "http://valve.github.io";
            return e.textBaseline = "top", e.font = '14px "Arial"', e.textBaseline = "alphabetic", e.fillS
        },
```

2. Sends computed fingerprint back to server

```
Request URL: http://us-west-2-v2-t.ztsrv.com/1/i/REMOVED;za/p.gif
```

https://github.com/disconnectme/disconnect-tracking-protection/blob/master/descriptions.md

Initial success: changing practices



→ This is a full-featured editor demo. Please explore! ←

TinyMCE is your best choice for building modern, internationalized and accessible content creation experiences.

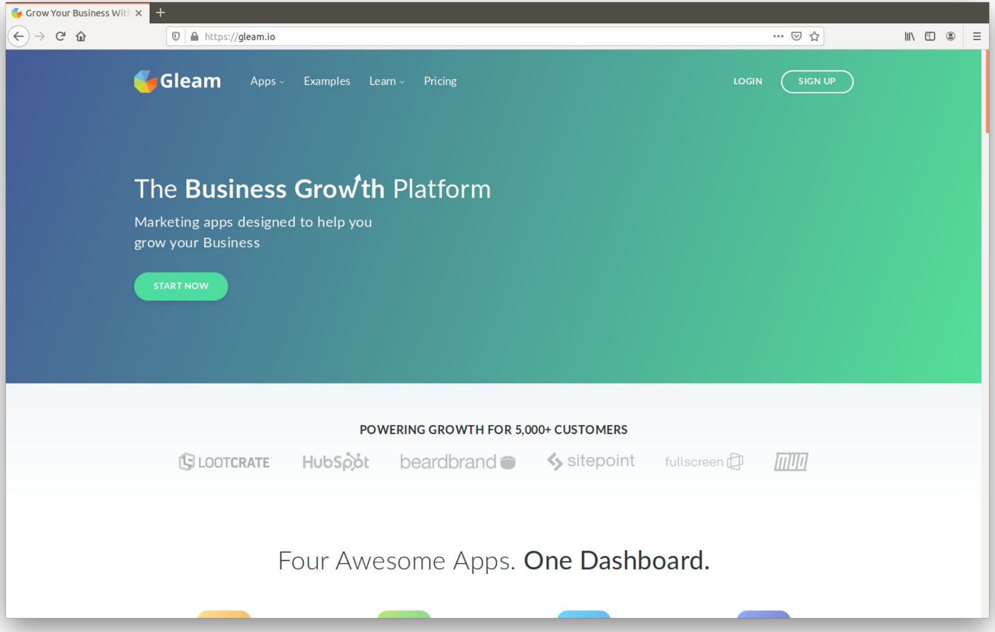
No matter what you're building, TinyMCE has got you covered.

🛠 50+ Plugins	💡 Premium Support	🖍 Custom Skins	⚙ Full API Access

TinyMCE removed fingerprint2js from their HTML Editor as a result of our blocking

https://bugzilla.mozilla.org/show_bug.cgi?id=1544159

Initial success: changing practices



The Business Growth Platform

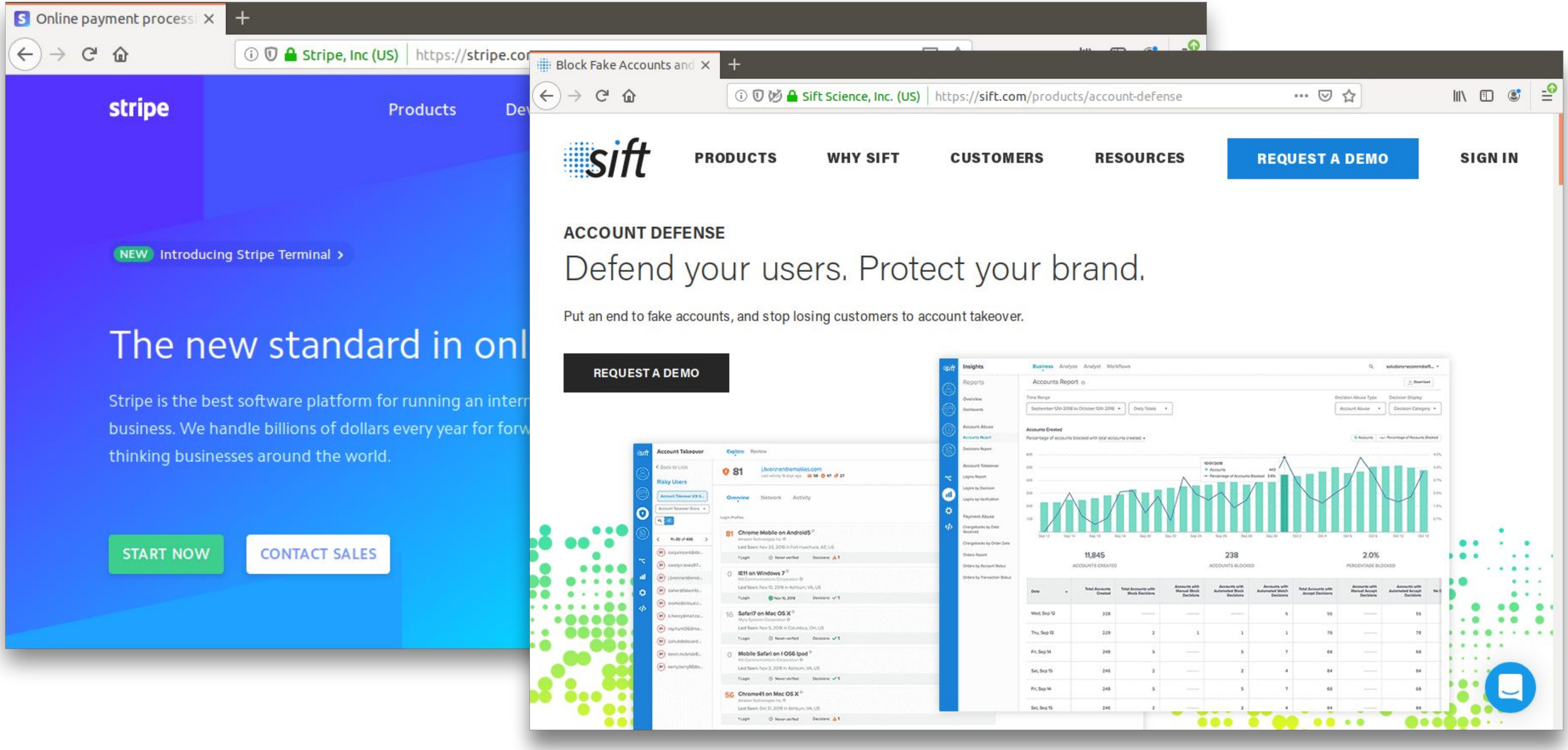
Marketing apps designed to help you grow your Business

Four Awesome Apps. One Dashboard.

Gleam moved fingerprinting script from gleam.io to fraudjs.io to avoid app breakage

https://bugzilla.mozilla.org/show_bug.cgi?id=1558658

Challenge: Fingerprinting for anti-fraud



Online payment process

Stripe, Inc (US) | https://stripe.co

stripe

Products

De

NEW Introducing Stripe Terminal ›

The new standard in onl

Stripe is the best software platform for running an intern business. We handle billions of dollars every year for forw thinking businesses around the world.

START NOW

CONTACT SALES

Block Fake Accounts and

Sift Science, Inc. (US) | https://sift.com/products/account-defense

sift

PRODUCTS

WHY SIFT

CUSTOMERS

RESOURCES

REQUEST A DEMO

SIGN IN

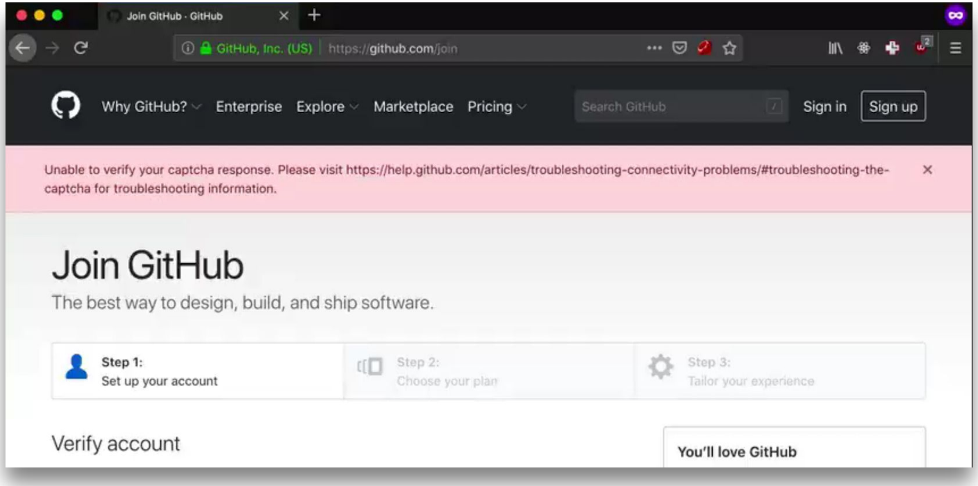
ACCOUNT DEFENSE

Defend your users. Protect your brand.

Put an end to fake accounts, and stop losing customers to account takeover.

REQUEST A DEMO

Blocking anti-fraud leads to major site breakage



Unable to verify your captcha response. Please visit https://help.github.com/articles/troubleshooting-connectivity-problems/#troubleshooting-the-captcha for troubleshooting information.

Join GitHub

The best way to design, build, and ship software.

Step 1: Set up your account

Step 2: Choose your plan

Step 3: Tailor your experience

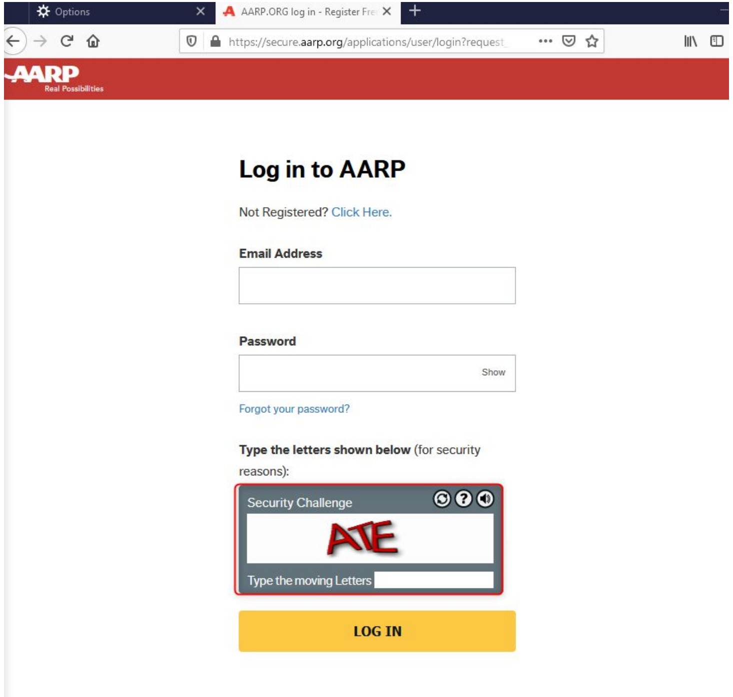
Verify account

You'll love GitHub

Github account creation broken when Arkose Labs captcha was blocked for fingerprinting

https://twitter.com/richgilbank/status/1090269987888082944

Blocking anti-fraud leads to major site breakage


Options
AARP.ORG log in - Register Fre
https://secure.aarp.org/applications/user/login?request
AARP
Real Possibilities

Log in to AARP

Not Registered? Click Here.

Email Address

Password

Show

Forgot your password?

Type the letters shown below (for security reasons):

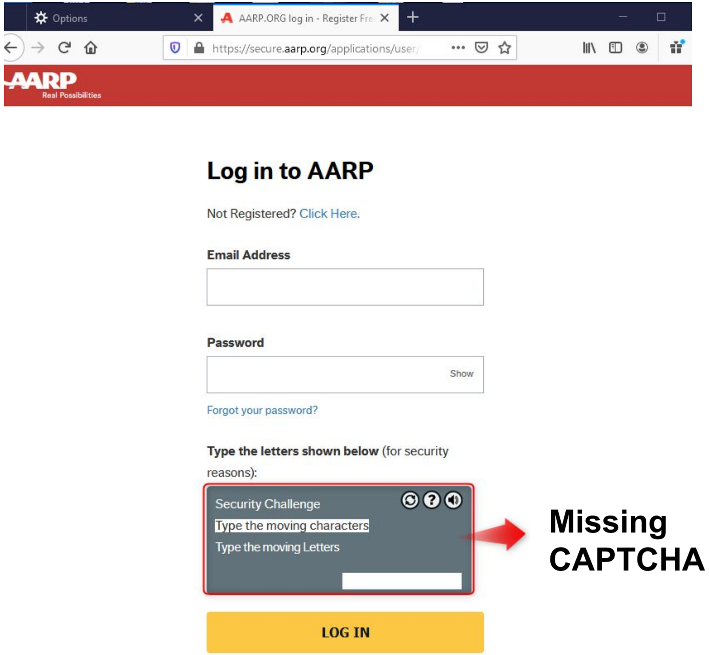
Security Challenge

ATE

Type the moving Letters

LOG IN

No Blocking


Options
AARP.ORG log in - Register Fre
https://secure.aarp.org/applications/user/
AARP
Real Possibilities

Log in to AARP

Not Registered? Click Here.

Email Address

Password

Show

Forgot your password?

Type the letters shown below (for security reasons):

Security Challenge

Type the moving characters

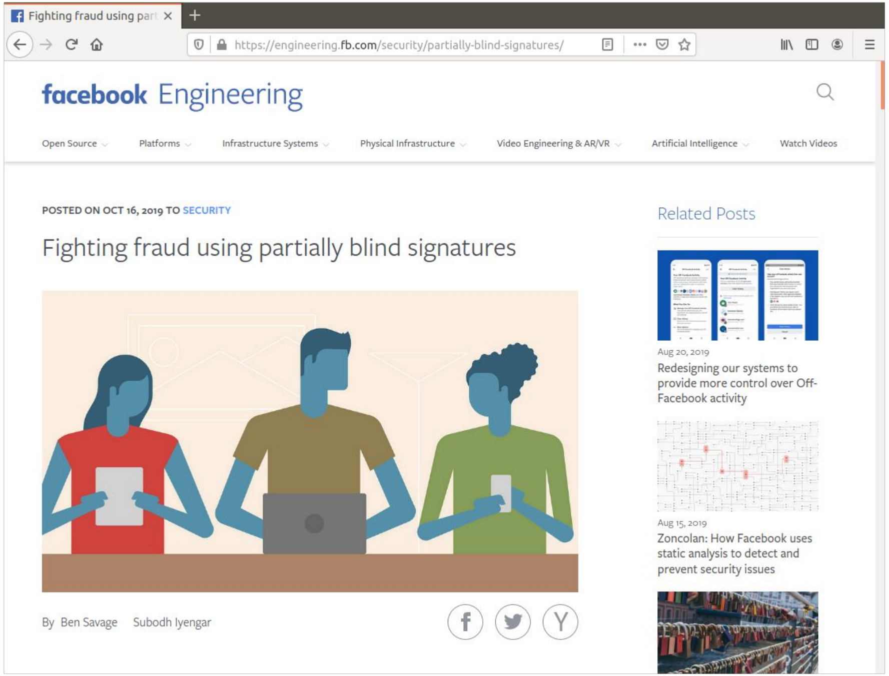
Type the moving Letters

LOG IN

Missing CAPTCHA

Blocking Fingerprinters

Two possible solutions to safer anti-fraud?



POSTED ON OCT 16, 2019 TO SECURITY

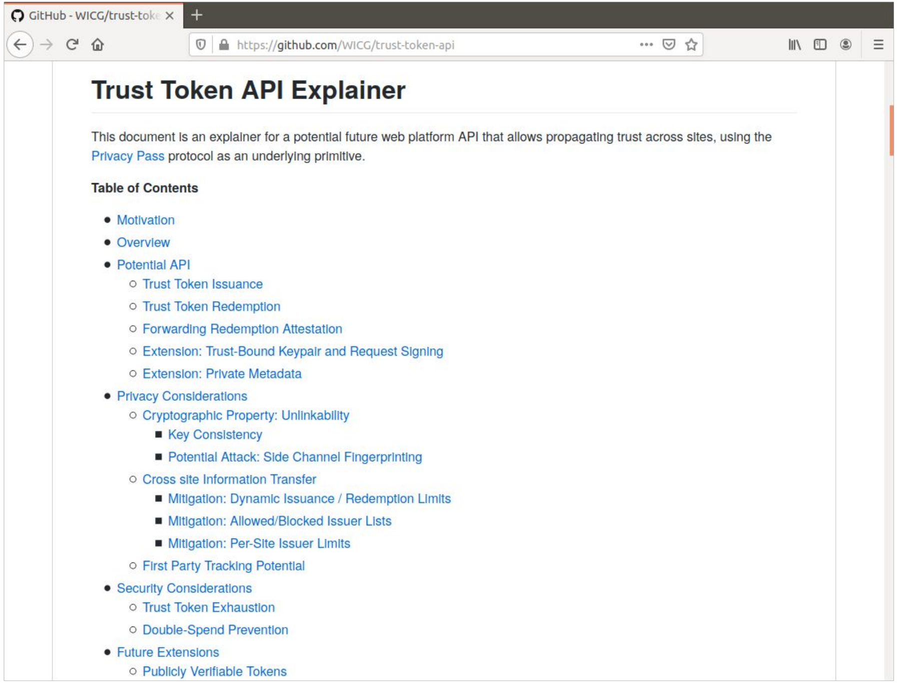
Fighting fraud using partially blind signatures

By Ben Savage Subodh Iyengar

Related Posts

Aug 20, 2019
Redesigning our systems to provide more control over Off-Facebook activity

Aug 15, 2019
Zoncolan: How Facebook uses static analysis to detect and prevent security issues

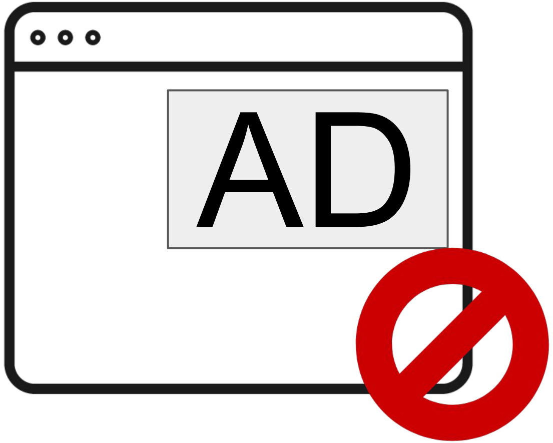


Trust Token API Explainer

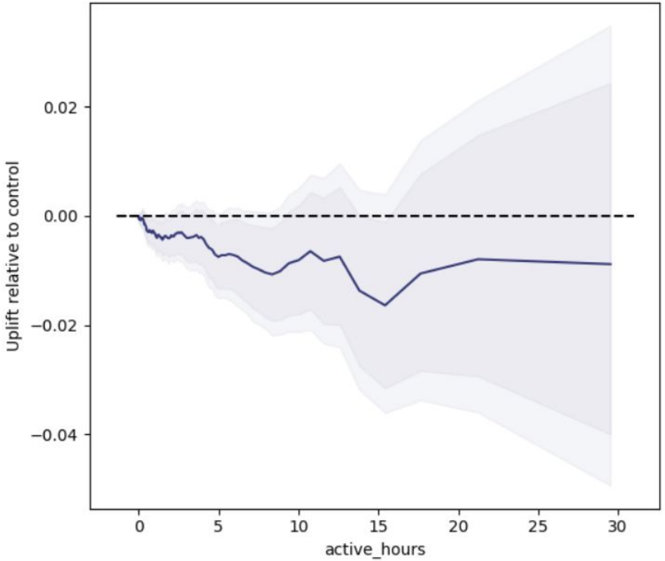
This document is an explainer for a potential future web platform API that allows propagating trust across sites, using the Privacy Pass protocol as an underlying primitive.

Table of Contents

Assume fraud is solved; can we block everything else?



Assume fraud is solved; can we block everything else?



… we tried that in a user study but we still saw 0.2% and 0.6% users leave Firefox because of it.

https://mozilla.report/post/projects/fingerprinting_protections.kp/

Why does blocking non-tracking fingerprinters cause users to leave Firefox?

¯_(ツ)_/¯

Challenge: discovering sites broken by our protections

Approach	**Problems**
User Reports	● Noisey ● Unreliable
User Studies	● Noisey ● No clear way to measure
Manual QA	● Limited scope ● Expensive: 1 month of full-time work per 1,000 sites
Automated Crawls	● Limited scope ● No clear way to measure

moz://a

Mozilla Research Grants 2019H2

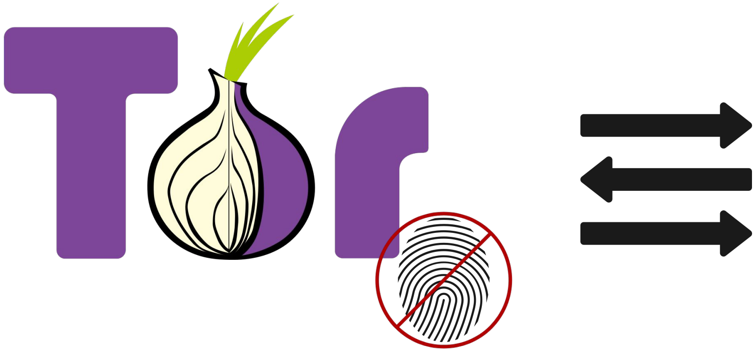
How can we automate the process of discovering broken sites?

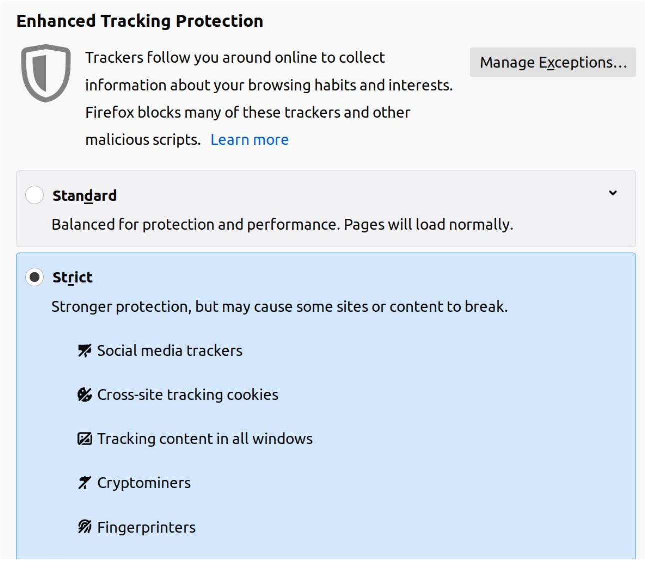
Amount: $40,000

Deadline
Friday, November 22nd at 2:22pm
Pacific Daylight Time (PDT)

https://mozilla-research.forms.fm/mozilla-research-grants-2019h2/forms/7376

A possible step forward for anti-fingerprinting?





Enhanced Tracking Protection

Trackers follow you around online to collect information about your browsing habits and interests. Firefox blocks many of these trackers and other malicious scripts. Learn more

○ **Standard**

Balanced for protection and performance. Pages will load normally.

● **Strict**

Stronger protection, but may cause some sites or content to break.

- Social media trackers
- Cross-site tracking cookies
- Tracking content in all windows
- Cryptominers
- Fingerprinters

Per-frame fingerprinting resistance based on a blocklist

https://bugzilla.mozilla.org/show_bug.cgi?id=1531873

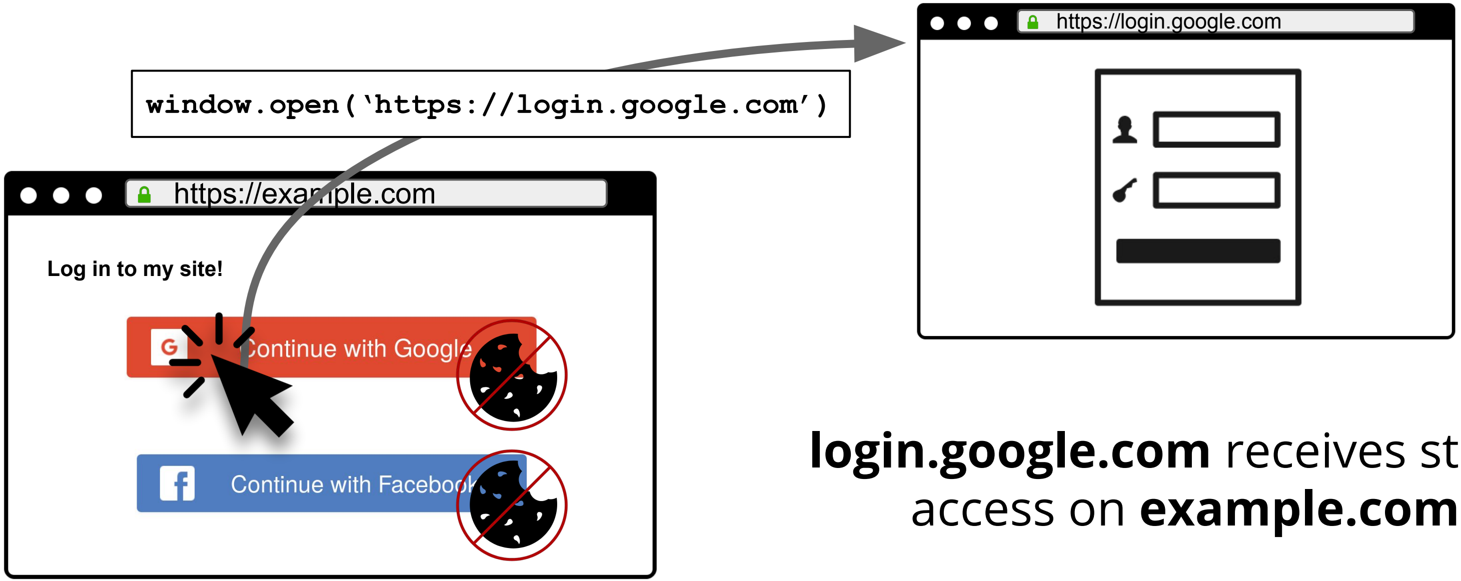
My asks for you:

1. Help us find technical alternatives to a global identifier for:
    a. Federated login
    b. Anti-fraud / device reputation
    c. Advertisement attribution / measurement
2. Find violations of our anti-tracking policies
    a. Name and shame
    b. We can update our blocks
3. Help us explore ways to better discover broken sites
    a. Apply to our grant!

THANK YOU!

BACKUP SLIDES

Interaction allows interactive embeds to work



https://login.google.com

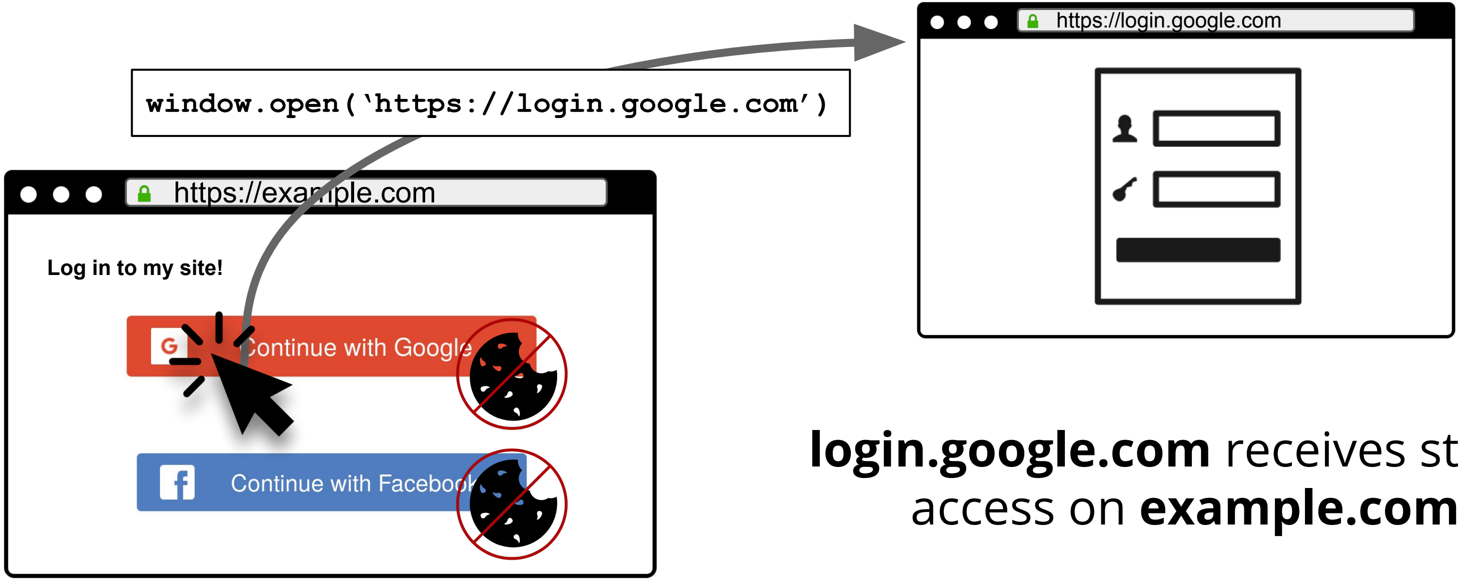
```
window.open('https://login.google.com')
```

https://example.com

Log in to my site!

login.google.com receives storage access on **example.com***

Interaction allows interactive embeds to work

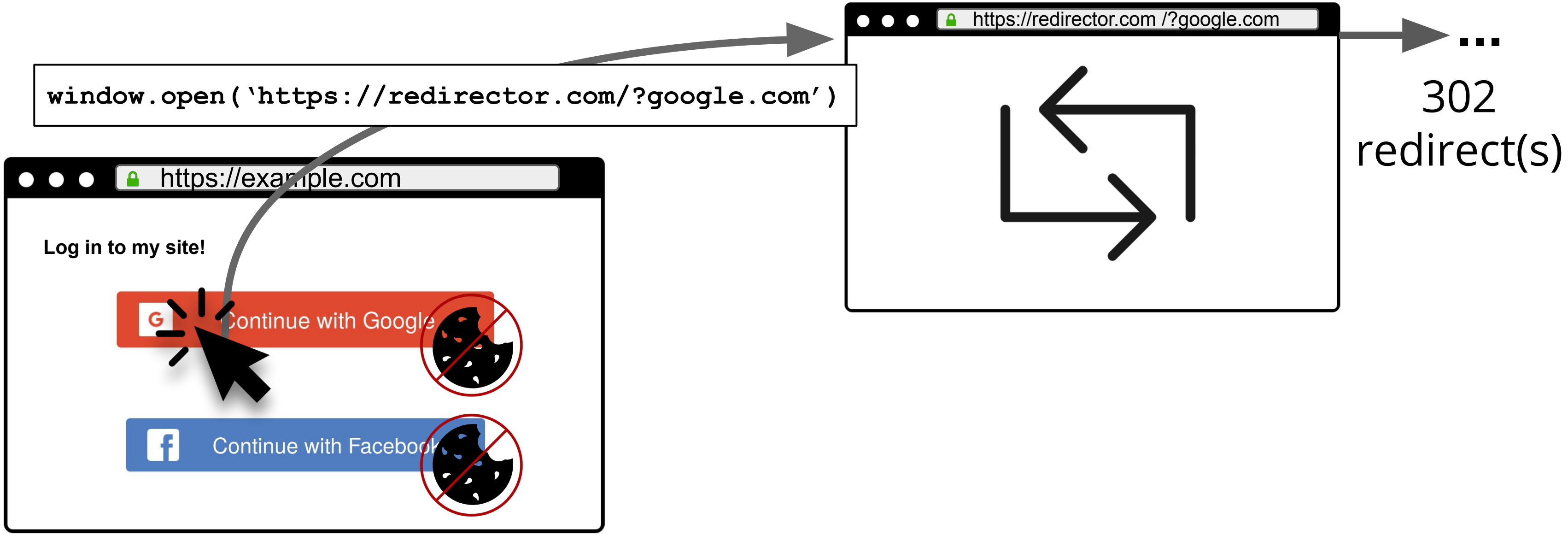


login.google.com receives storage access on **example.com***

** Provided it meets some additional requirements.*

See: https://developer.mozilla.org/en-US/docs/Mozilla/Firefox/Privacy/Storage_access_policy

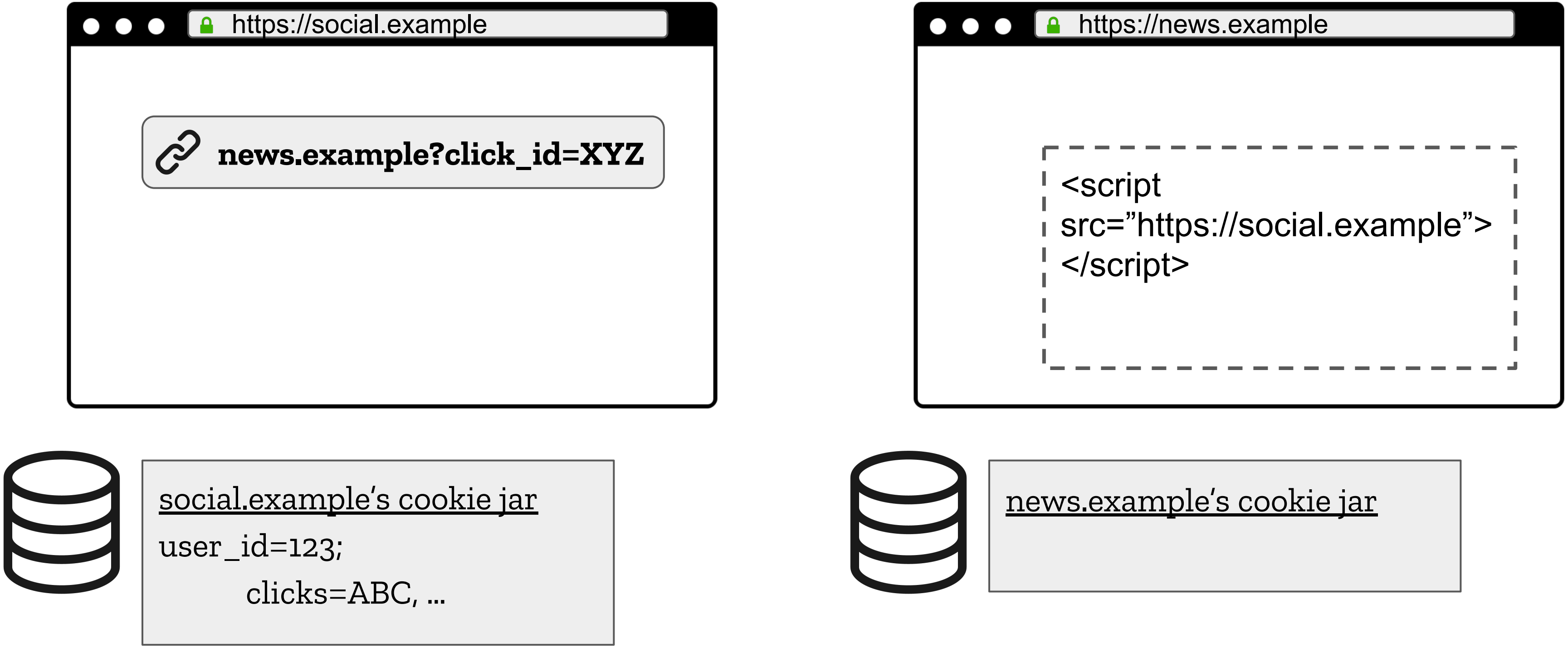
We also handle redirects...



```
window.open('https://redirector.com/?google.com')
```

See: https://developer.mozilla.org/en-US/docs/Mozilla/Firefox/Privacy/Storage_access_policy

A workaround: Cross-site tracking with query strings



news.example?click_id=XYZ

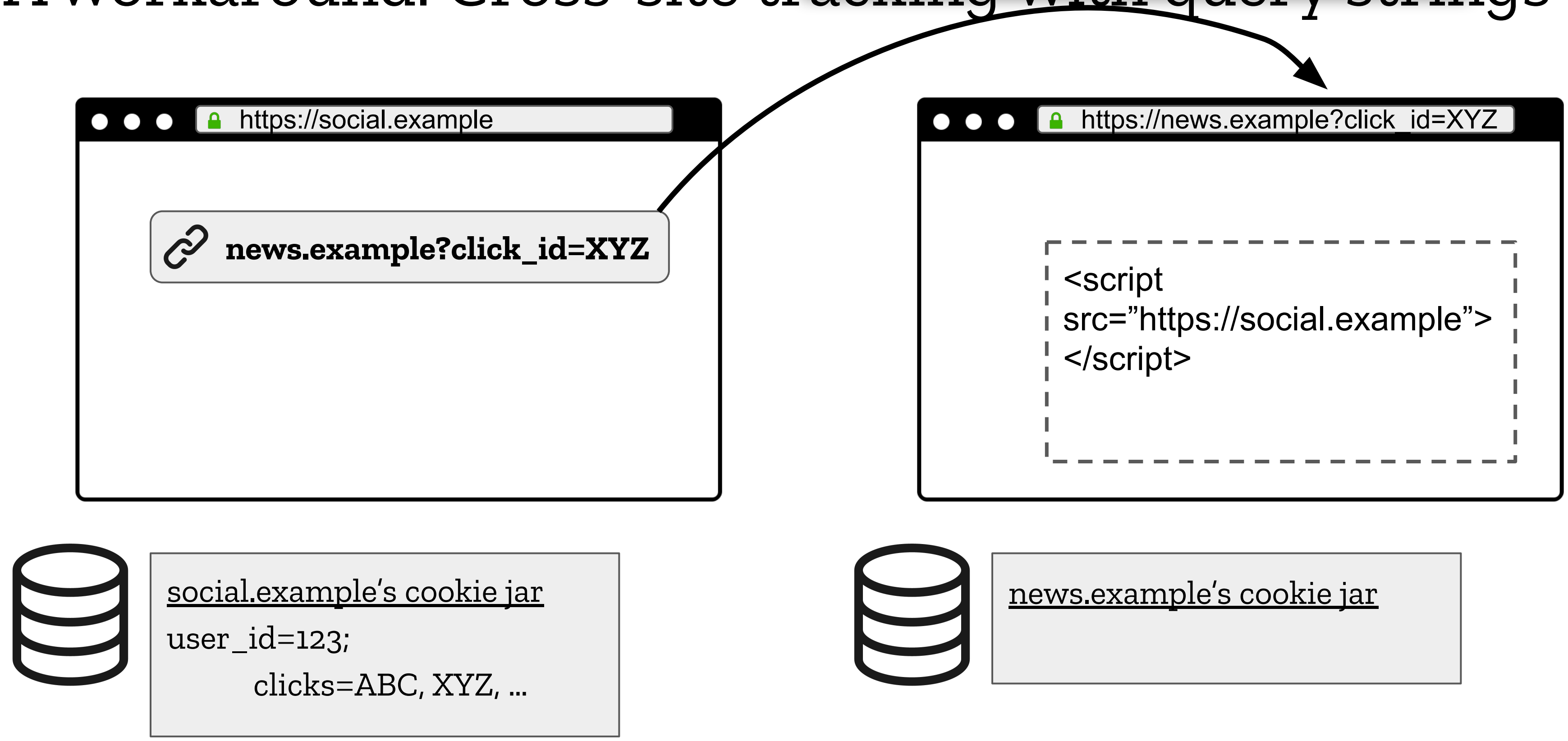
```
<script
src=”https://social.example”>
</script>
```

social.example’s cookie jar

user_id=123;
clicks=ABC, ...

news.example’s cookie jar

A workaround: Cross-site tracking with query strings



(1) Append unique id in click_id parameter

```
<script
src=”https://social.example”>
</script>
```

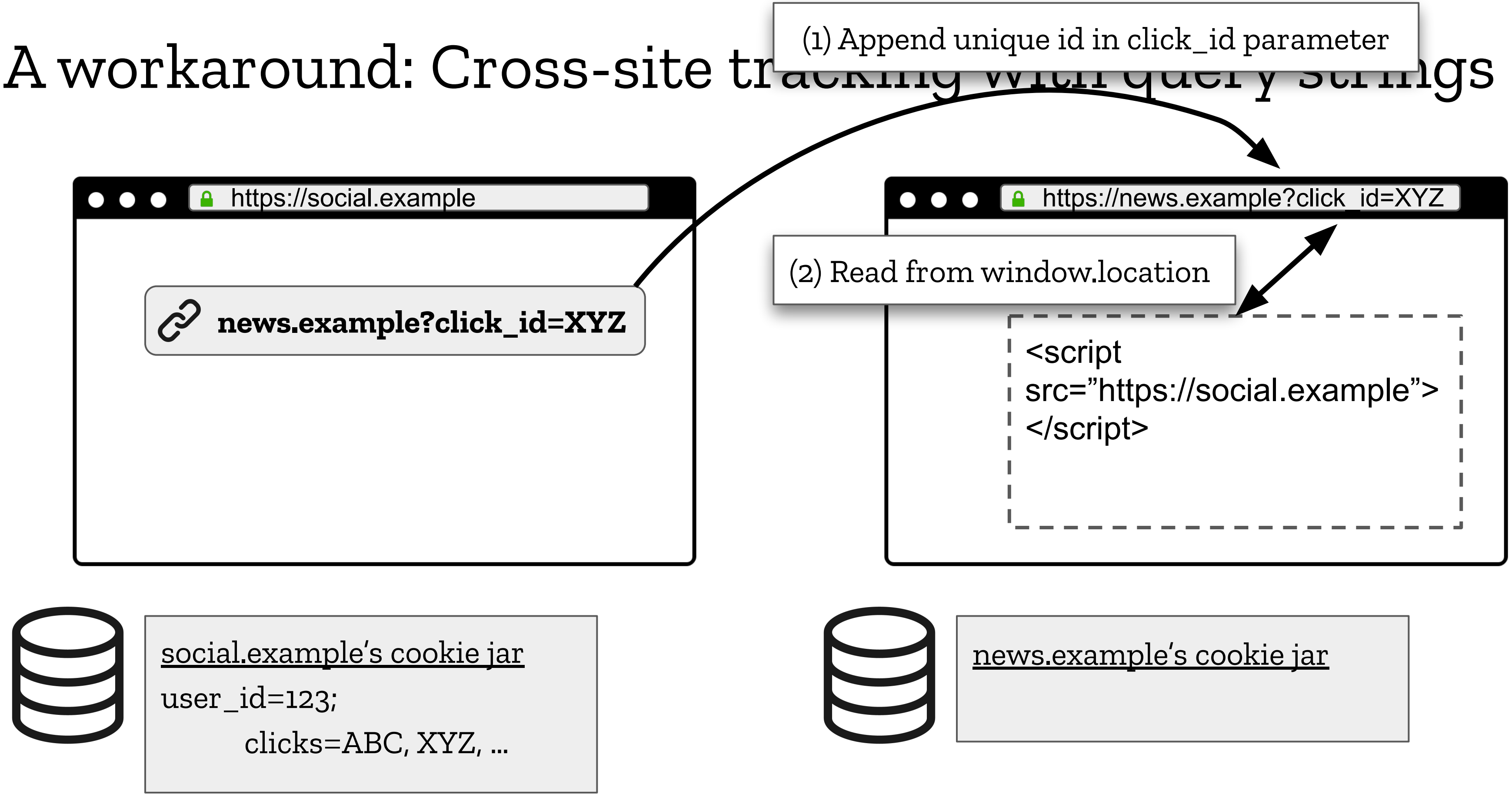
social.example’s cookie jar

user_id=123;

clicks=ABC, XYZ, ...

news.example’s cookie jar

A workaround: Cross-site tracking with query strings



(1) Append unique id in click_id parameter

https://social.example

news.example?click_id=XYZ

https://news.example?click_id=XYZ

(2) Read from window.location

```
<script
src=”https://social.example”>
</script>
```

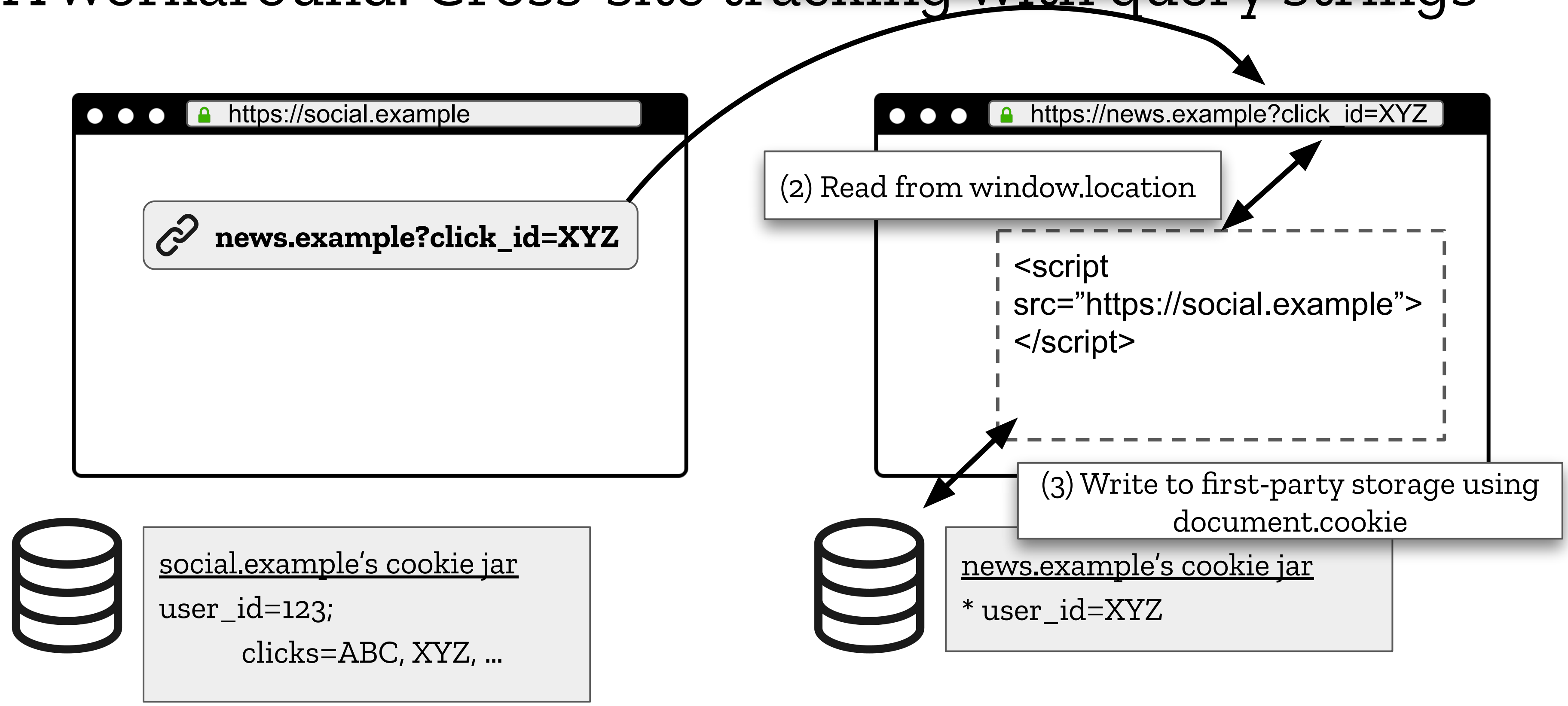
social.example's cookie jar

user_id=123;

clicks=ABC, XYZ, ...

news.example's cookie jar

A workaround: Cross-site tracking with query strings



(1) Append unique id in click_id parameter

(2) Read from window.location

```
<script
src=”https://social.example”>
</script>
```

(3) Write to first-party storage using document.cookie

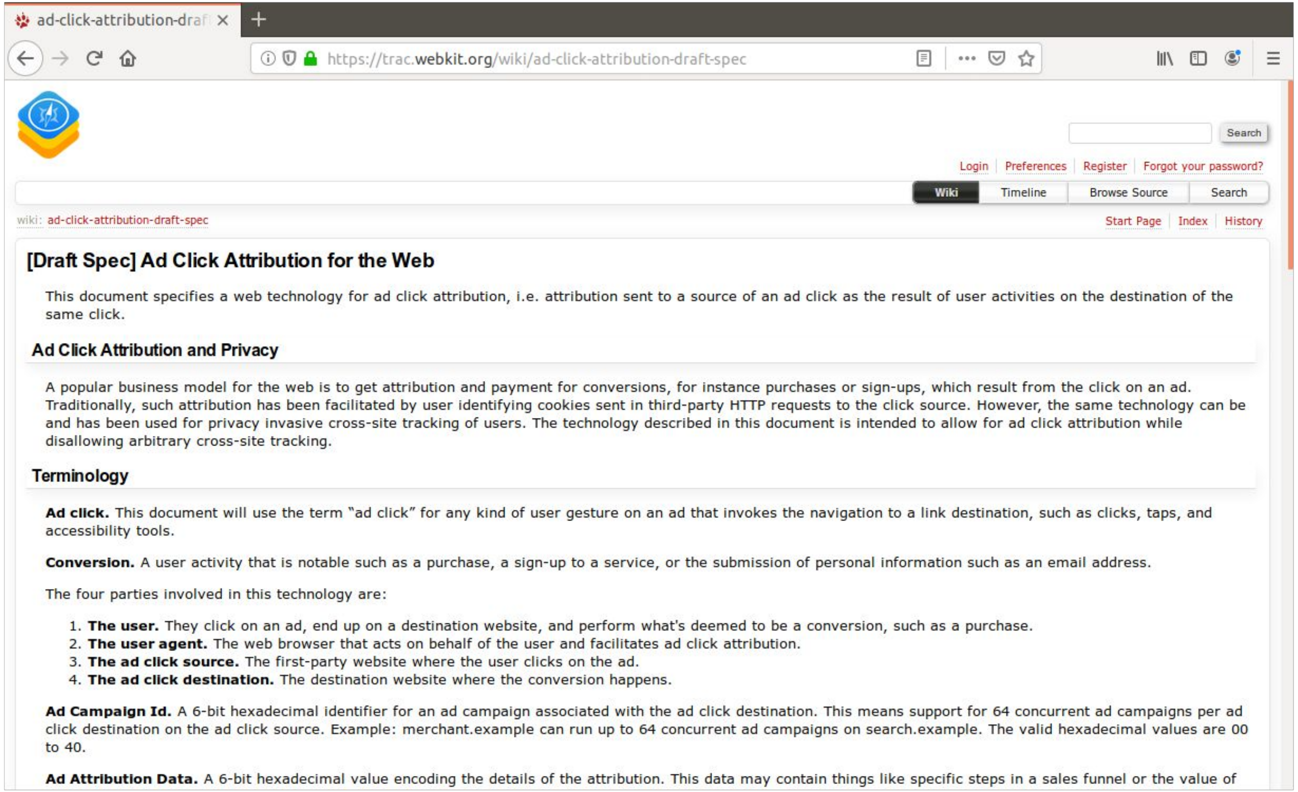
social.example’s cookie jar

user_id=123;
clicks=ABC, XYZ, ...

news.example’s cookie jar

* user_id=XYZ

Request: a safer way to do ad measurement



ad-click-attribution-draf
https://trac.webkit.org/wiki/ad-click-attribution-draft-spec
Search
Login | Preferences | Register | Forgot your password?
Wiki | Timeline | Browse Source | Search
wiki: ad-click-attribution-draft-spec
Start Page | Index | History

[Draft Spec] Ad Click Attribution for the Web

This document specifies a web technology for ad click attribution, i.e. attribution sent to a source of an ad click as the result of user activities on the destination of the same click.

Ad Click Attribution and Privacy

A popular business model for the web is to get attribution and payment for conversions, for instance purchases or sign-ups, which result from the click on an ad. Traditionally, such attribution has been facilitated by user identifying cookies sent in third-party HTTP requests to the click source. However, the same technology can be and has been used for privacy invasive cross-site tracking of users. The technology described in this document is intended to allow for ad click attribution while disallowing arbitrary cross-site tracking.

Terminology

Ad click. This document will use the term "ad click" for any kind of user gesture on an ad that invokes the navigation to a link destination, such as clicks, taps, and accessibility tools.

Conversion. A user activity that is notable such as a purchase, a sign-up to a service, or the submission of personal information such as an email address.

The four parties involved in this technology are:

1. **The user.** They click on an ad, end up on a destination website, and perform what's deemed to be a conversion, such as a purchase.
2. **The user agent.** The web browser that acts on behalf of the user and facilitates ad click attribution.
3. **The ad click source.** The first-party website where the user clicks on the ad.
4. **The ad click destination.** The destination website where the conversion happens.

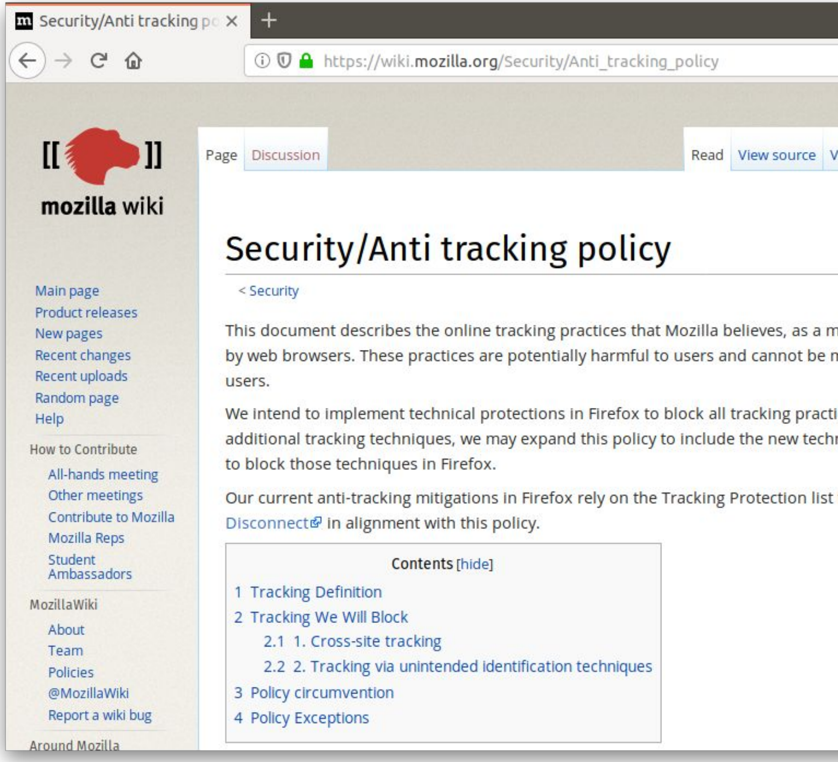
Ad Campaign Id. A 6-bit hexadecimal identifier for an ad campaign associated with the ad click destination. This means support for 64 concurrent ad campaigns per ad click destination on the ad click source. Example: merchant.example can run up to 64 concurrent ad campaigns on search.example. The valid hexadecimal values are 00 to 40.

Ad Attribution Data. A 6-bit hexadecimal value encoding the details of the attribution. This data may contain things like specific steps in a sales funnel or the value of

Challenge: Fingerprinting for anti-fraud

Policy exceptions:

1. Improving client authentication
2. Preventing the creation of fraudulent accounts
3. Preventing the completion of fraudulent purchases.



Security/Anti tracking policy

< Security

This document describes the online tracking practices that Mozilla believes, as a m by web browsers. These practices are potentially harmful to users and cannot be m users.

We intend to implement technical protections in Firefox to block all tracking practi additional tracking techniques, we may expand this policy to include the new techn to block those techniques in Firefox.

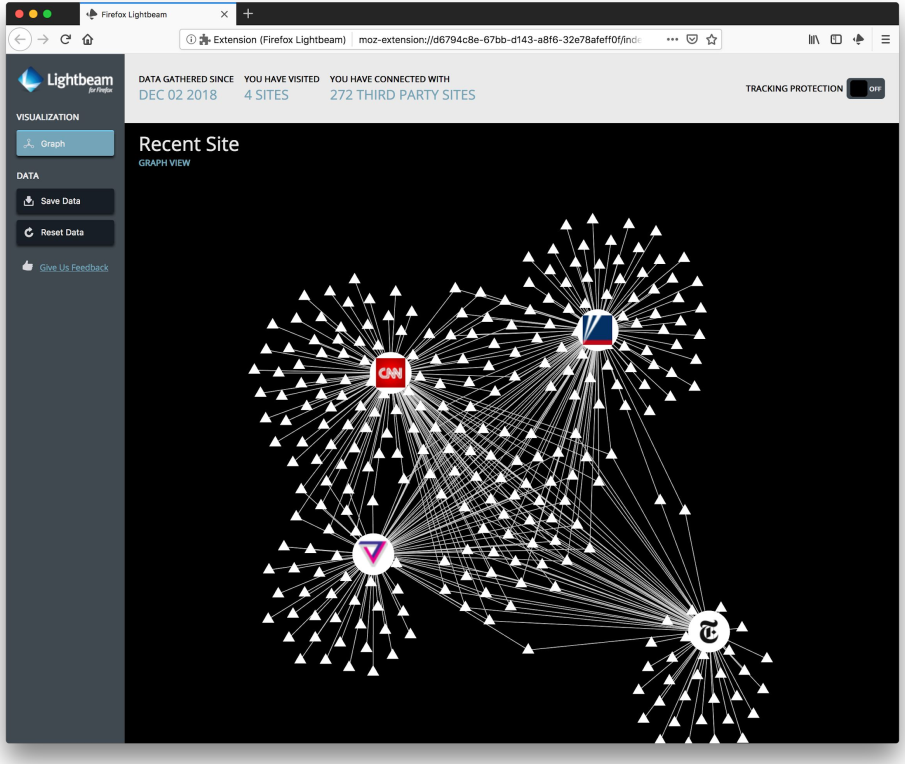
Our current anti-tracking mitigations in Firefox rely on the Tracking Protection list Disconnect in alignment with this policy.

Contents [hide]

The web needs **default-on** tracking protection …

4 news sites

272 third parties



Extension (Firefox Lightbeam) moz-extension://d6794c8e-67bb-d143-a8f6-32e78afeff0f/inde

DATA GATHERED SINCE DEC 02 2018

YOU HAVE VISITED 4 SITES

YOU HAVE CONNECTED WITH 272 THIRD PARTY SITES

TRACKING PROTECTION OFF

Recent Site

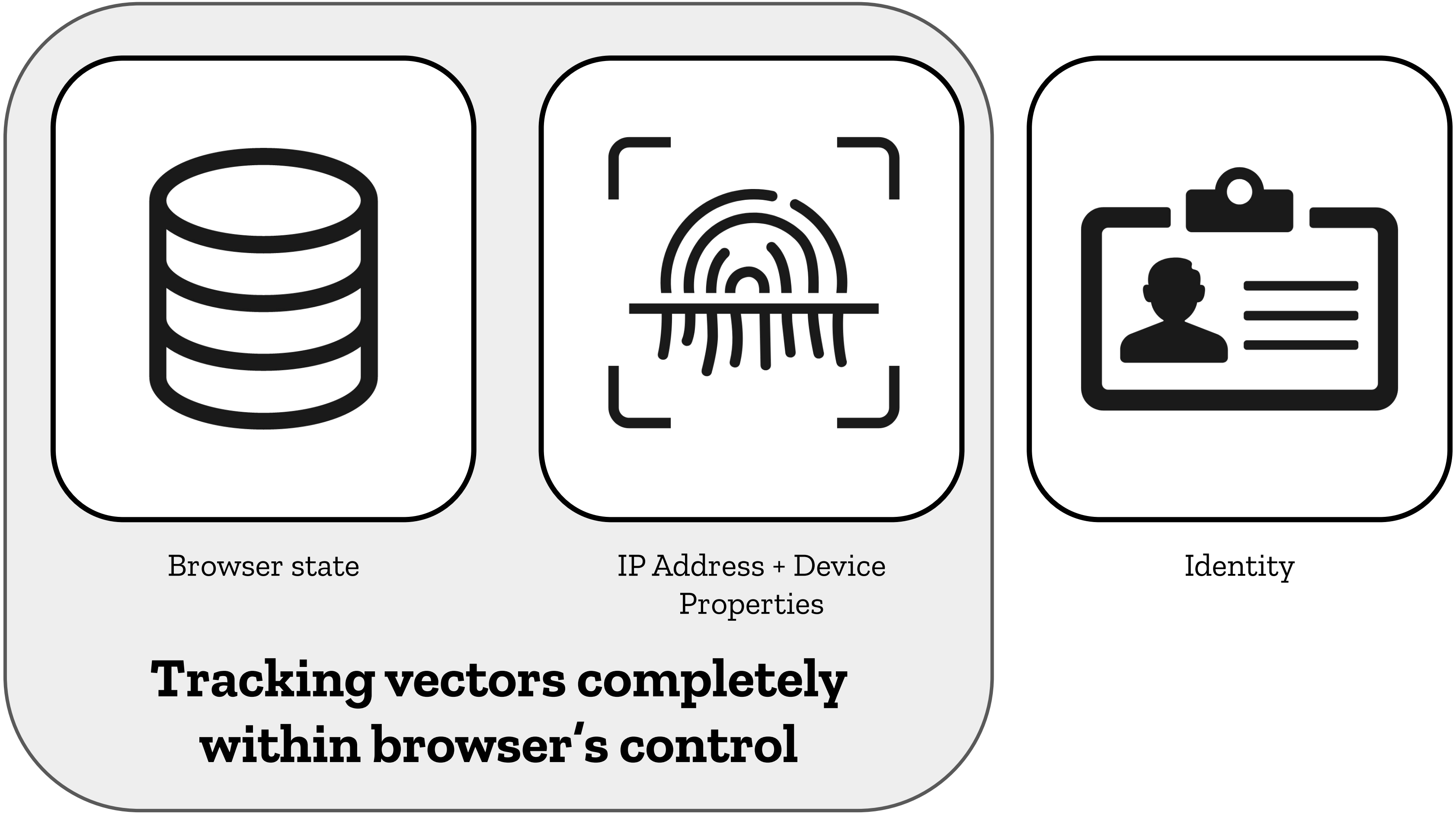
GRAPH VIEW

The web needs **default-on** tracking protection …
… and not just from third-party cookies

Browser state

IP Address + Device Properties

Identity



Browser state

IP Address + Device Properties

Identity

Tracking vectors completely within browser's control

The tracking landscape

Browser state

IP Address + Device Properties

Identity

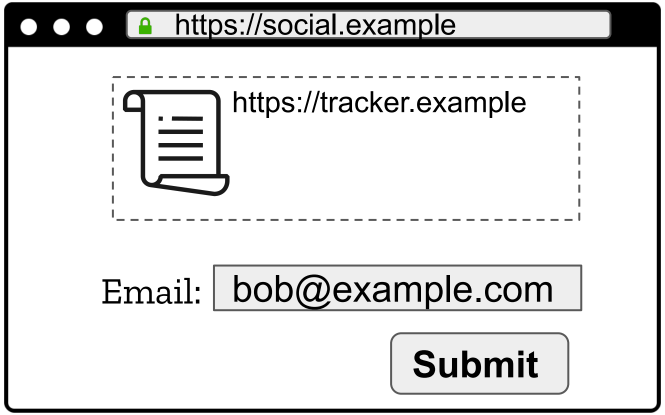
The tracking landscape

Browser state

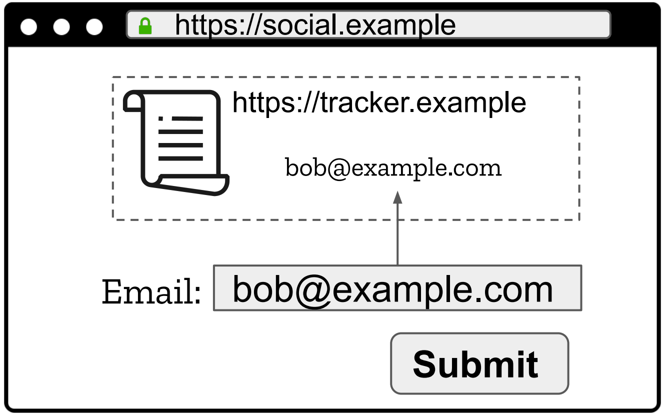
IP Address + Device Properties

Identity

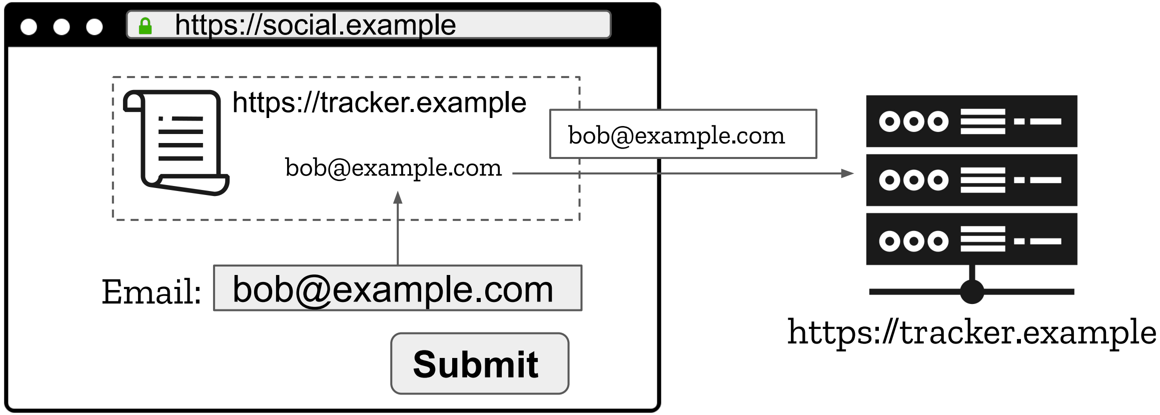
Scripts can collect PII for tracking



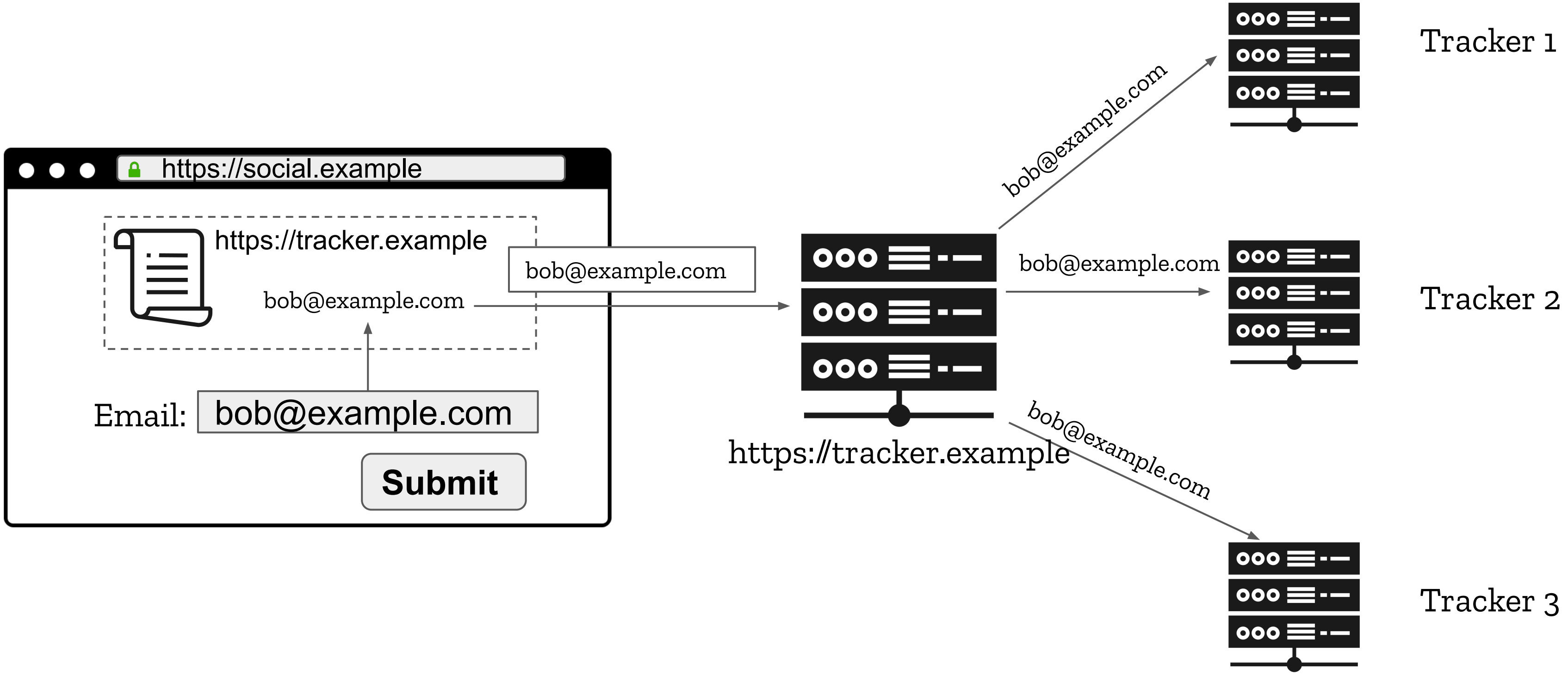
Scripts can collect PII for tracking



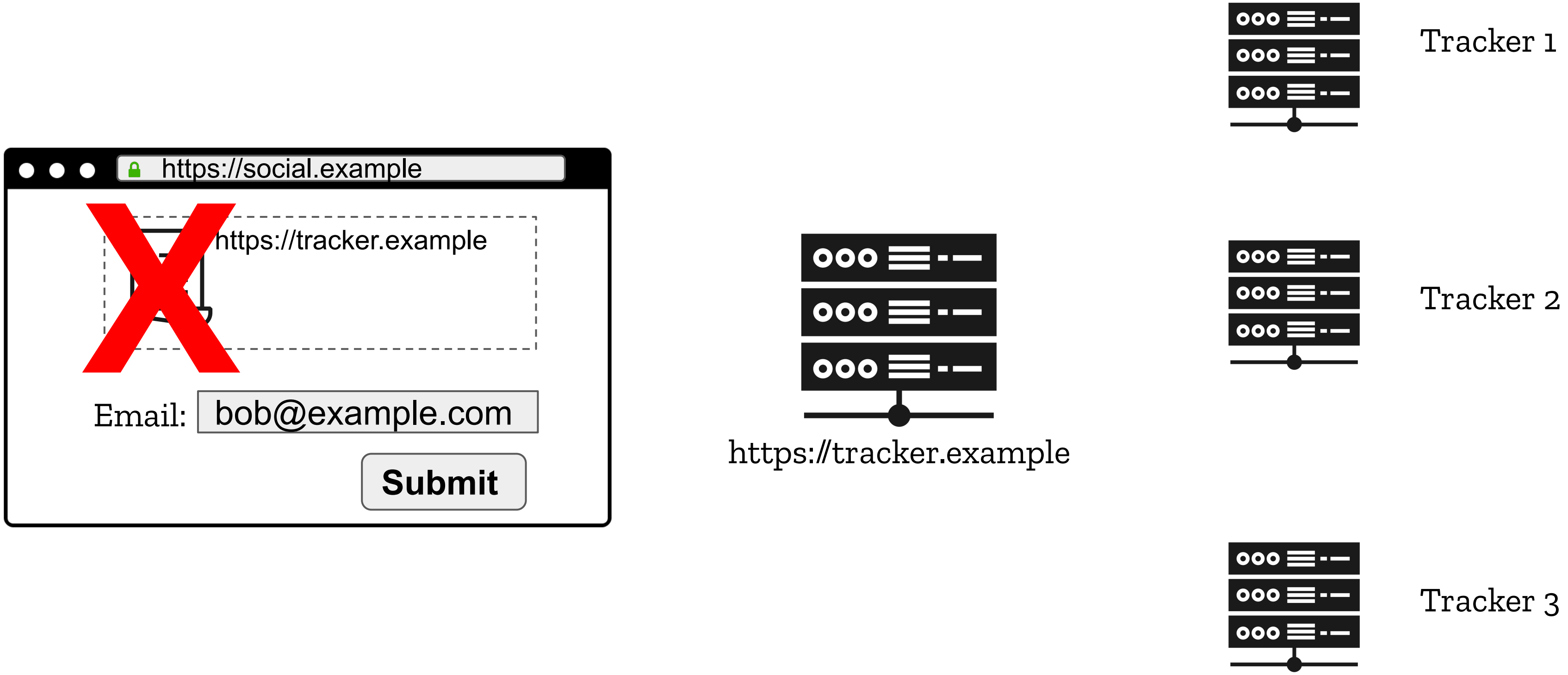
Scripts can collect PII for tracking



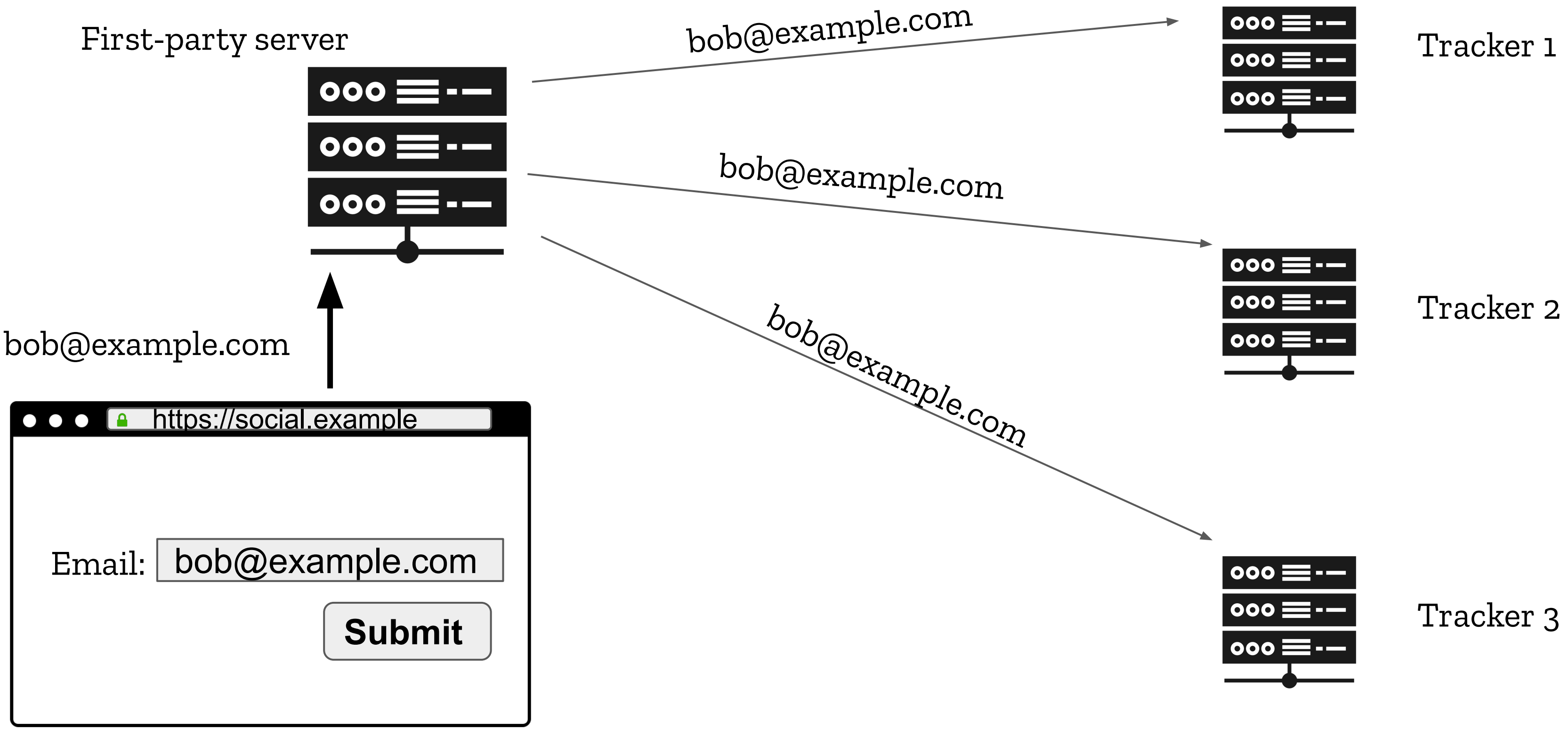
Scripts can collect PII for tracking



We can block scripts that scrape PII



In-browser protection options are limited...



First-party server

bob@example.com

Tracker 1

bob@example.com

Tracker 2

bob@example.com

Tracker 3

bob@example.com

https://social.example

Email: bob@example.com

Submit

The tracking landscape

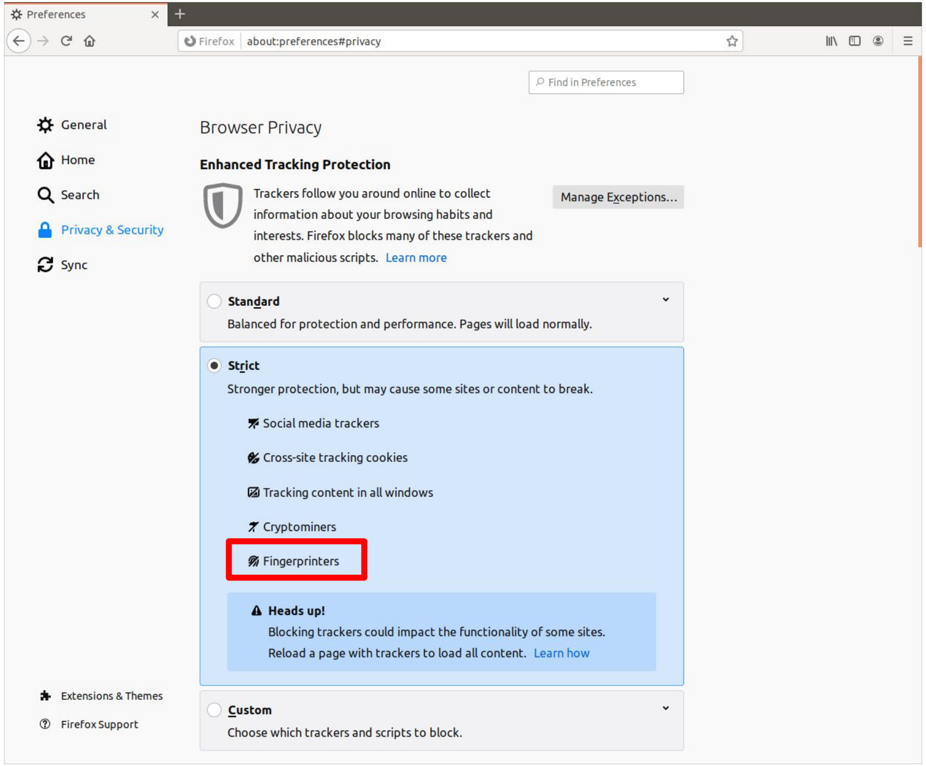
Browser state

IP Address + Device Properties

Identity

Fingerprinting blocking available since Firefox 67

Firefox 70



Browser Privacy

Enhanced Tracking Protection

Trackers follow you around online to collect information about your browsing habits and interests. Firefox blocks many of these trackers and other malicious scripts. Learn more

Manage Exceptions…

○ **Standard**
Balanced for protection and performance. Pages will load normally.

● **Strict**
Stronger protection, but may cause some sites or content to break.

- Social media trackers
- Cross-site tracking cookies
- Tracking content in all windows
- Cryptominers
- Fingerprinters

Heads up!
Blocking trackers could impact the functionality of some sites.
Reload a page with trackers to load all content. Learn how

○ **Custom**
Choose which trackers and scripts to block.

How can we prevent identity-based tracking?

Request: a safer way to do anti-fraud