

a set of data that can be used to detect operating systems, protocols, software, and hardware of a tech stack.

# **Brave, Fingerprinting and Privacy on the Web**

# Me (the early years)

- **Grew up in Chicago**  
...actual Chicago
- **Law school, then freelance web design**  
Started: Anchorage, AK  
Ended: Judge Judy Show invitation
- **PhD in Computer Science**  
University of Illinois at Chicago

# Me, now

- **Privacy Researcher at Brave**  
Research to improve privacy in the browser
- **Co-Chair of PING**  
Privacy reviews of new web standards
- **Academic Collaborator**  
“Pure” research

# Brave in a Slide

- Privacy focused
- Alternative funding model for the web
- Research and engineering focused
- Browsers and infrastructure now, more to come...



# Overview

1. Why websites track (and how much)
2. “Classic” tracking
3. Fingerprinting / “passive tracking”
4. Fingerprinting counter measures
5. Anti-finger printing exercise
6. Privacy protections in Brave
7. Wrapping up

# Overview

- 1. Why websites track (and how much)**
2. “Classic” tracking
3. Fingerprinting / “passive tracking”
4. Fingerprinting counter measures
5. Anti-finger printing exercise
6. Privacy protections in Brave
7. Wrapping up

# Why Does Tracking Exist?





Taylor's one-day mission

From JOHN ETHERIDGE

JAMES TAYLOR can prove he is up to being England's permanent one-day captain after getting chosen to lead the new generation.

The 25-year-old batsman, takes charge against Ireland on May 8 — the first 50-over match since the World Cup disaster.

Regular skipper Eoin Morgan will again go to play in the IPL.

He had a nightmare World Cup and, if Taylor impresses, the selectors might think: 'The most likely long-term prospect, though, is Joe Root.'

Notts star Taylor said:

"We must put the World Cup behind us and not ignore it but learn from it. This is a fresh start."

England's 11-man squad has five uncapped players: Kent keeper/batsman Sam Billings, Surrey all-rounder Zafar Ansari, Somerset seamer Liam Gregory, Northants all-rounder David Willey and Hampshire batsman James Vince.

More players may be added after England pick their Third Test XI to face West Indies on Friday.

Take a look: Taylor (left), Vince, Ansari, Billings (MC), Willey (MC), Gregory, Willey, Finn.

Kid Dan's ton of fun

TEENAGER Dan Lawrence upstaged Kevin Pietersen by becoming one of county cricket's youngest centurions.

The 17-year-old hit 161 in only his second first-class fixture as Essex racked up 610-8 against Surrey at The Oval.

Kids' Geoffrey Bryan in 1920 and Dilip Patel for Worcestershire in 1976 are believed to have hit tons when younger than Lawrence, whose previous highest was 95.

KP was eight not out as Surrey won by 175 runs in their second innings.

Lee: Oui will return

By JOHNNY FORDHAM

LEE DICKSON believes English rugby can wrest back control from teams across the Channel.

A French invasion takes place in Toulouse on Saturday as Clermont face Toulon in the European Champions Cup final.

Dickson's Premiership leaders Northampton were NOT'd by Clermont in the English scrum-half, 30, said: "We will be back."

"In the past we have beaten the big French teams — and Wasps nearly turned Toulon over."

# Captaincy is wrong Root

**IT WOULD BE A ROAD TO RUIN**

**VIEW TO A DILL**

**ANDREW DILLON**

**BRIGHTON'S summer transfer policy may have to take a hit after chairman Tom Bloom's set of misfortunes.**

**The Seagulls supreme placed £13,000 on himself to finish the Brighton Marathon in no more than 45 minutes — only to cross the line four minutes and 38 seconds later.**

**RONNIE O'SULLIVAN** is known as the school of science but they have been turning their hands to amateur drama.

Reporters were gathered to interview Gareth Barry when the subject of last night's Ross County inevitably surfaced, seeing as it is the ONLY interesting topic of conversation.

As soon as Barkley's name was mentioned, the club's subtle press officer came out with a contrite apology, staged concern — as in 'be careful here mate, tricky subject'.

But the carefully-managed plan to thwart the nasty hacks backfired when the entire group fell silent and he was presented with a packet of throat lozenges at the next press conference.

**JOE ROOT** has become a world-class batsman, averaging more than 100 in Test cricket in the past year.

But to make him England captain any time in the next five years would be a disaster. I think it would ruin him as a batsman.

Like a few players before him, Joe has been handed the mantle of ICC Future English Captain.

Everyone expects it is going to happen and I've little doubt he will lead England at some point. But I would pray it doesn't happen for at least five years, by which time he will be only 29.

In fact I'm not sure Joe will ever be a good captain because it just doesn't suit his character.

Joe has a natural cheeky chappy personality, he's a joker, a jester, a wind-up merchant and a general breath of fresh air around the dressing room.

To be captain, he would need to change and become more mature and perhaps even a bit more serious. That simply is not Joe.

Of course, there is no vacancy at the moment anyway because Alastair Cook is doing a fine job as is back concentrating on Test cricket. Cooky won't still be captain in five years' time, so I suppose don't give the job to Joe.

Just let Joe Root bat at No 5 and score hundred after hundred and then let England's Steve Waugh. So don't think about moving him up the order, either.

I love the way Joe handles himself on the field. He has

## Graeme Swann

OUR COLUMNISTS ARE

THE TALK OF SPORT

JOE ROOT has become a world-class batsman, averaging more than 100 in Test cricket in the past year.

But to make him England captain any time in the next five years would be a disaster. I think it would ruin him as a batsman.

Like a few players before him, Joe has been handed the mantle of ICC Future English Captain.

Everyone expects it is going to happen and I've little doubt he will lead England at some point. But I would pray it doesn't happen for at least five years, by which time he will be only 29.

In fact I'm not sure Joe will ever be a good captain because it just doesn't suit his character.

Joe has a natural cheeky chappy personality, he's a joker, a jester, a wind-up merchant and a general breath of fresh air around the dressing room.

To be captain, he would need to change and become more mature and perhaps even a bit more serious. That simply is not Joe.

Of course, there is no

vacancy at the moment anyway because Alastair Cook is doing a fine job as is back concentrating on Test cricket. Cooky won't still be captain in five years' time, so I suppose don't give the job to Joe.

Just let Joe Root bat at No 5 and score hundred after hundred and then let England's Steve Waugh. So don't think about moving him up the order, either.

I love the way Joe handles himself on the field. He has

the only big difference is about how you think about the game with the pressure, the spotlight and TV coverage.

It is a mental thing, what makes you better or worse.

And Joe's head is full of calmness, confidence and positive thoughts right now.

In fact, he comes from the start that Joe had great talent and temperament.

He doesn't really sledge. It would be like being sledged to take the heat out of what he looks. Nobody could take him seriously.

Joe is great at smiling to take the heat out of situations. There's nothing more annoying for a steaming, sweating Neanderthal fast bowler than having some kid smiling and winking back at him.

But don't be fooled — Joe has a streak of steel, too.

He has been hitting national centuries in the past 14 months without being a tough cookie.

He has discovered the secret of Test cricket very early.

The ball is the same size, the pitch the same length as you've played against in county cricket. Joe realised

about Joe's batting is the crease, about how he brings to the crease.

He walks in like an神经元 puppy, playing 100 shots before he's ten yards on to the outfield.

He has positive intent and urgency from the start and it gradually perks up the rest of the team.

Every other batsman in the Second Test in Grenada was hitting 50s, but Joe had a strike-rate of 50 runs per 100 balls but Joe rattled off 100 not out from 229 balls.

I want to see a way batsmen play spin bowling and Joe always looks to score runs against spin.

A lot of attention is given to a bad ball before attacking.

So Joe forces spinners to be more loose stuff, especially a wrist-spinner like Davenдра Bishto. He played Bishto magnificently.

The new Geoffrey Boycott — the Yorkshireshire who scores all the runs and runs everyone out — has certainly cashed in since he and his last five Test centuries have been 180, 200 not out and not out, 140 not out and 140 not out. Daren Sammy hundreds, as Graham Gooch called them. The best thing

I kept trying to hit the spinners over the top, then Joe tried something similar and won consistently.

He has certainly cashed in since he and his last five Test centuries have been 180, 200 not out and not out, 140 not out and 140 not out. Daren Sammy

hundreds, as Graham Gooch

called them. The best thing

I kept trying to hit the spinners over the top, then Joe tried something similar and won consistently.

He has certainly cashed in since he and his last five Test centuries have been 180, 200 not out and not out, 140 not out and 140 not out. Daren Sammy

hundreds, as Graham Gooch

called them. The best thing

I kept trying to hit the spinners over the top, then Joe tried something similar and won consistently.

He has certainly cashed in since he and his last five Test centuries have been 180, 200 not out and not out, 140 not out and 140 not out. Daren Sammy

hundreds, as Graham Gooch

called them. The best thing

I kept trying to hit the spinners over the top, then Joe tried something similar and won consistently.

He has certainly cashed in since he and his last five Test centuries have been 180, 200 not out and not out, 140 not out and 140 not out. Daren Sammy

hundreds, as Graham Gooch

called them. The best thing

I kept trying to hit the spinners over the top, then Joe tried something similar and won consistently.

He has certainly cashed in since he and his last five Test centuries have been 180, 200 not out and not out, 140 not out and 140 not out. Daren Sammy

hundreds, as Graham Gooch

called them. The best thing

I kept trying to hit the spinners over the top, then Joe tried something similar and won consistently.

He has certainly cashed in since he and his last five Test centuries have been 180, 200 not out and not out, 140 not out and 140 not out. Daren Sammy

hundreds, as Graham Gooch

called them. The best thing

I kept trying to hit the spinners over the top, then Joe tried something similar and won consistently.

He has certainly cashed in since he and his last five Test centuries have been 180, 200 not out and not out, 140 not out and 140 not out. Daren Sammy

hundreds, as Graham Gooch

called them. The best thing

I kept trying to hit the spinners over the top, then Joe tried something similar and won consistently.

He has certainly cashed in since he and his last five Test centuries have been 180, 200 not out and not out, 140 not out and 140 not out. Daren Sammy

hundreds, as Graham Gooch

called them. The best thing

I kept trying to hit the spinners over the top, then Joe tried something similar and won consistently.

He has certainly cashed in since he and his last five Test centuries have been 180, 200 not out and not out, 140 not out and 140 not out. Daren Sammy

hundreds, as Graham Gooch

called them. The best thing

I kept trying to hit the spinners over the top, then Joe tried something similar and won consistently.

He has certainly cashed in since he and his last five Test centuries have been 180, 200 not out and not out, 140 not out and 140 not out. Daren Sammy

hundreds, as Graham Gooch

called them. The best thing

I kept trying to hit the spinners over the top, then Joe tried something similar and won consistently.

He has certainly cashed in since he and his last five Test centuries have been 180, 200 not out and not out, 140 not out and 140 not out. Daren Sammy

hundreds, as Graham Gooch

called them. The best thing

I kept trying to hit the spinners over the top, then Joe tried something similar and won consistently.

He has certainly cashed in since he and his last five Test centuries have been 180, 200 not out and not out, 140 not out and 140 not out. Daren Sammy

hundreds, as Graham Gooch

called them. The best thing

I kept trying to hit the spinners over the top, then Joe tried something similar and won consistently.

He has certainly cashed in since he and his last five Test centuries have been 180, 200 not out and not out, 140 not out and 140 not out. Daren Sammy

hundreds, as Graham Gooch

called them. The best thing

I kept trying to hit the spinners over the top, then Joe tried something similar and won consistently.

He has certainly cashed in since he and his last five Test centuries have been 180, 200 not out and not out, 140 not out and 140 not out. Daren Sammy

hundreds, as Graham Gooch

called them. The best thing

I kept trying to hit the spinners over the top, then Joe tried something similar and won consistently.

He has certainly cashed in since he and his last five Test centuries have been 180, 200 not out and not out, 140 not out and 140 not out. Daren Sammy

hundreds, as Graham Gooch

called them. The best thing

I kept trying to hit the spinners over the top, then Joe tried something similar and won consistently.

He has certainly cashed in since he and his last five Test centuries have been 180, 200 not out and not out, 140 not out and 140 not out. Daren Sammy

hundreds, as Graham Gooch

called them. The best thing

I kept trying to hit the spinners over the top, then Joe tried something similar and won consistently.

He has certainly cashed in since he and his last five Test centuries have been 180, 200 not out and not out, 140 not out and 140 not out. Daren Sammy

hundreds, as Graham Gooch

called them. The best thing

I kept trying to hit the spinners over the top, then Joe tried something similar and won consistently.

He has certainly cashed in since he and his last five Test centuries have been 180, 200 not out and not out, 140 not out and 140 not out. Daren Sammy

hundreds, as Graham Gooch

called them. The best thing

I kept trying to hit the spinners over the top, then Joe tried something similar and won consistently.

He has certainly cashed in since he and his last five Test centuries have been 180, 200 not out and not out, 140 not out and 140 not out. Daren Sammy

hundreds, as Graham Gooch

called them. The best thing

I kept trying to hit the spinners over the top, then Joe tried something similar and won consistently.

He has certainly cashed in since he and his last five Test centuries have been 180, 200 not out and not out, 140 not out and 140 not out. Daren Sammy

hundreds, as Graham Gooch

called them. The best thing

I kept trying to hit the spinners over the top, then Joe tried something similar and won consistently.

He has certainly cashed in since he and his last five Test centuries have been 180, 200 not out and not out, 140 not out and 140 not out. Daren Sammy

hundreds, as Graham Gooch

called them. The best thing

I kept trying to hit the spinners over the top, then Joe tried something similar and won consistently.

**100%**  
**FREE**

**MAGAZINE  
SUBSCRIPTIONS!**





## Welcome to The "First" Banner Ad

Yes, this site is supposed to look this way. After all, this is what most web pages looked like back on October 27, 1994 -- the day that Wired Magazine flipped the switch on its first website, hotwired.com, starting a revolution in web content and advertising that still reverberates today.

This site is dedicated to showing off one of the ads that ran on that site. No, it wasn't the "first" as there were a handful of other ads that ran on various sections of hotwired.com. This site is also here to tell the story of how that ad came to be, how it succeeded beyond anything we had imagined, and how we tried to set an example for how corporations could communicate with their audiences.

This site launched on October 27, 2014. It is being constantly updated, so please check back again soon for more. In the meantime, get started by clicking your mouse in the banner ad above explore these other options:



[Previous](#) | [Next](#) | [Random](#) | [List Sites](#)

Chicago Tribune: Chicago news, X +

chicagotribune.com

SECTIONS SEARCH ENEWSPAPER WEATHER NEWSLETTERS BEST REVIEWS \$2 FOR 20 WEEKS SALE ENDS 11/4 LOG IN

CPS STRIKE IS OFFICIALLY ON AS CHICAGO TEACHERS UNION SAYS THERE IS NO LAST-MINUTE DEAL X

TOP LOCAL NEWS SOURCE OCTOBER 16, 2019 51°F

BREAKING NEWS SPORTS BUSINESS POLITICS OPINION ENTERTAINMENT

ADVERTISEMENT

HSBC

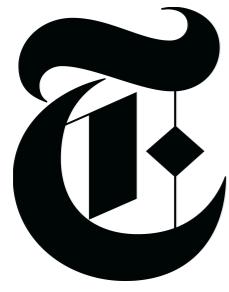
CPS STRIKE IS ON MORE CPS STRIKE COVERAGE >

CPS strike live updates: Chicago teachers reject city offer, will walk off job Thursday

Chicago Park District workers reach contract

SPECIAL SALE ONLY \$2 FOR 20 WEEKS Get stories that impact you SAVE NOW

Waiting for securepubads.g.doubleclick.net...



# The World's Worst Website

Gratuitous use of frames is a common mistake of web designers.

Many older browsers do not support frames. They disrupt the flow of the website and can be difficult to anticipate where a page may appear when a link is clicked. [Click here](#) for an example of a frames page which is opening in the wrong window. Use your browser's 'Back' button to escape.

Check out these links to websites whose opinions about frames is self evident:

[The "I Hate Frames" Frames Page](#)

Another [I Hate Frames Page](#)

[The International I Hate Frames Club](#)

[Why Frames Suck \(Most of the Time\)](#)

Angelfire Build your own FREE website at Angelfire.com Share: del.icio.us | digg | reddit | Twitter | facebook

Marketing is more fun WHEN YOU SMASH STUFF

VIEW THE WORK

Ads by Google

site!

## Welcome to the World's Worst Website!

This web was designed to graphically demonstrate the most common mistakes made by new Web Page designers.

*Where am I and where are the links to other pages?*

An easy to use navigation structure is essential to any well designed website!  
Important information should never be more than 2 clicks away.

As you can see, this text is difficult to read. There needs to more contrast between the background color and the text color. [Here's another example](#) of a poor choice of a background/ text color and size.

Keep your backgrounds simple. White or light colors usually work best. Your background should not compete with the content of the page for the users attention. If you would like to use a background picture, select a picture that uses muted colors or format your picture as a watermark. Select text colors which will contrast well with the background picture.

Constantly running animations can be distracting when used excessively.



# CHICAGO SUN-TIMES

\$ \$ \$

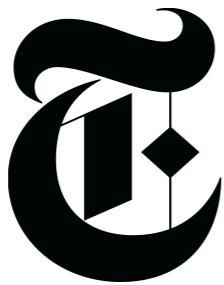


¢ ¢ ¢

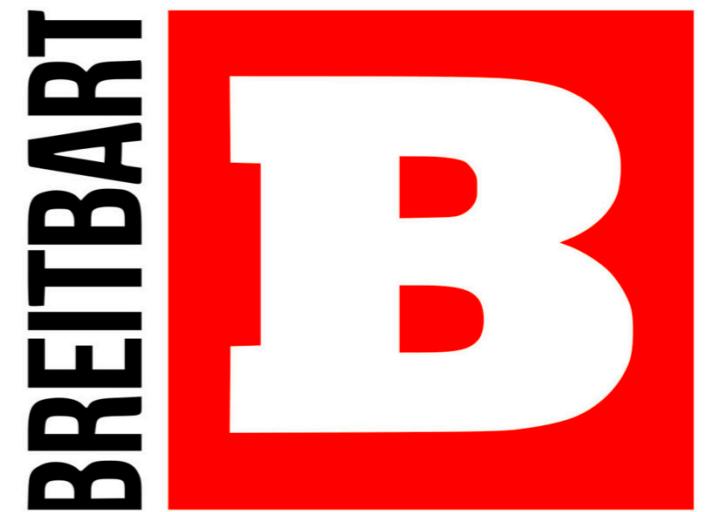


# CHICAGO SUN-TIMES





**Identify “expensive”  
people here**



**Pay a little to advertise  
to them here**

F How Target Figured Out A Te x

www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/

FREE REPORT: Top 10 Stocks for 2013

Log in | Sign up | Connect | Help

Forbes • New Posts • Most Popular • Lists • Video

Best Cover Letter Ever? 30 Under 30 You Need A Flu Shot

Search companies, people and lists

62.8k f Share 13.7k Tweet 5.6k in Share 353 SU Submit 3.5k g +1 1.9k reddit

Kashmir Hill, Forbes Staff  
Welcome to The Not-So Private Parts where technology & privacy collide  
+ Follow (1,089) f Follow 174k

TECH | 2/16/2012 @ 11:02AM | 1,913,626 views

# How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

307 comments, 167 called-out + Comment Now + Follow Comments

Every time you go shopping, you share intimate details about your consumption patterns with retailers. And many of those retailers are studying those details to figure out what you like, what you need, and which coupons are most likely to make you happy. [Target](#), for example, has figured out how to data-mine its way into your womb, to figure out whether you have a baby on the way long before you need to start buying diapers.



TARGET

Click here to see how Covidien is making a difference >



COVIDIEN

# DISPLAY LUMAscape

M  
A  
R  
K  
E  
T  
E  
R

C  
O  
N  
S  
U  
M  
E  
R



**But how much...**

# Online Tracking: A 1-million-site Measurement and Analysis

Steven Englehardt  
Princeton University  
ste@cs.princeton.edu

Arvind Narayanan  
Princeton University  
arvindn@cs.princeton.edu

## ABSTRACT

We present the largest and most detailed measurement of online tracking conducted to date, based on a crawl of the top 1 million websites. We make 15 types of measurements on each site, including stateful (cookie-based) and stateless (fingerprinting-based) tracking, the effect of browser privacy tools, and the exchange of tracking data between different sites (“cookie syncing”). Our findings include multiple sophisticated fingerprinting techniques never before measured in the wild.

This measurement is made possible by our open-source web privacy measurement tool, OpenWPM<sup>1</sup>, which uses an automated version of a full-fledged consumer browser. It supports parallelism for speed and scale, automatic recovery from failures of the underlying browser, and comprehensive browser instrumentation. We demonstrate our platform’s strength in enabling researchers to rapidly detect, quantify, and characterize emerging online tracking behaviors.

## 1. INTRODUCTION

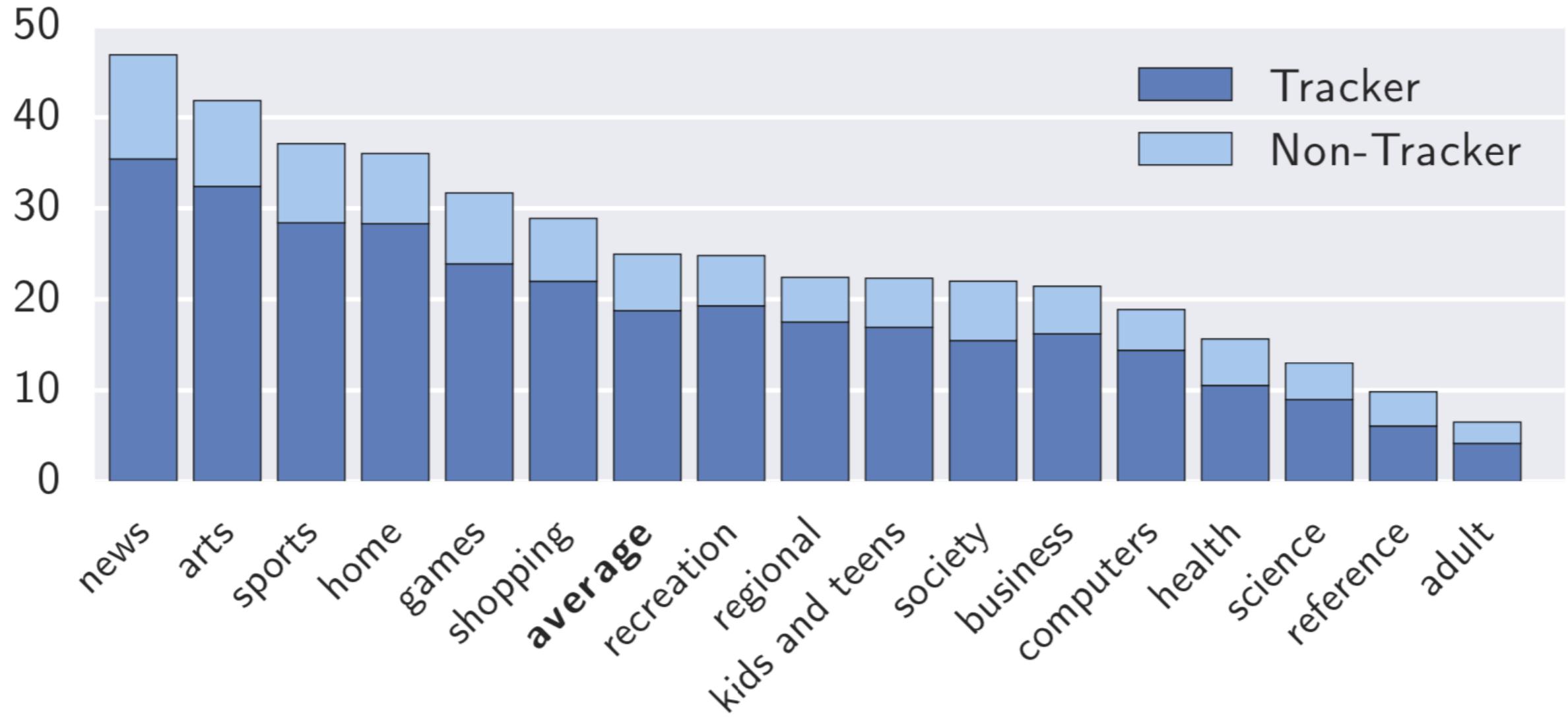
Web privacy measurement — observing websites and services to detect, characterize and quantify privacy-impacting behaviors — has repeatedly forced companies to improve

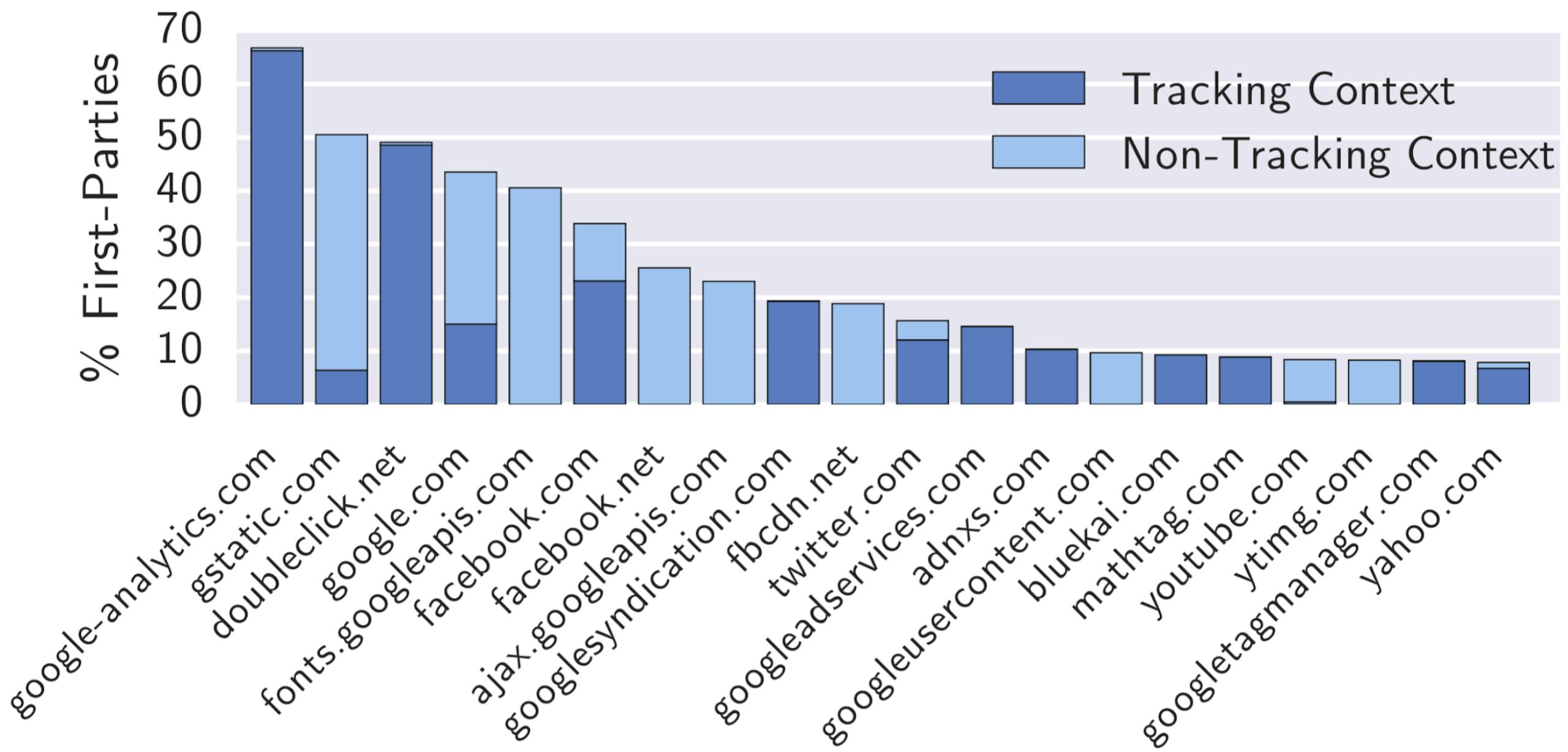
to resort to a stripped-down browser [31] (a limitation we explore in detail in Section 3.3). (2) We provide comprehensive instrumentation by expanding on the rich browser extension instrumentation of FourthParty [33], without requiring the researcher to write their own automation code. (3) We reduce duplication of work by providing a modular architecture to enable code re-use between studies.

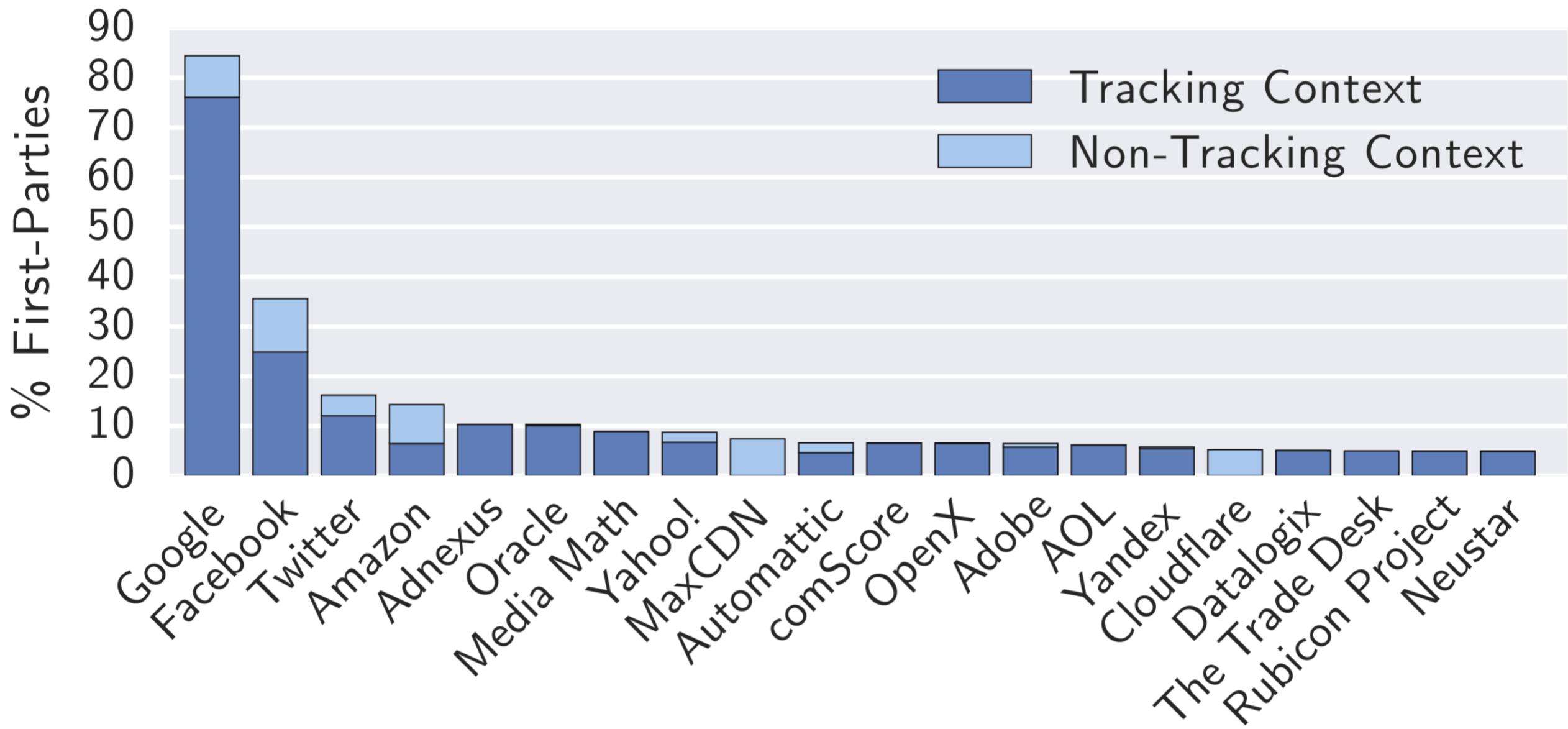
Solving these problems is hard because the web is not designed for automation or instrumentation. Selenium,<sup>2</sup> the main tool for automated browsing through a full-fledged browser, is intended for developers to test their *own* websites. As a result it performs poorly on websites not controlled by the user and breaks frequently if used for large-scale measurements. Browsers themselves tend to suffer memory leaks over long sessions. In addition, *instrumenting* the browser to collect a variety of data for later analysis presents formidable challenges. For full coverage, we’ve found it necessary to have three separate measurement points: a network proxy, a browser extension, and a disk state monitor. Further, we must link data collected from these disparate points into a uniform schema, duplicating much of the browser’s own internal logic in parsing traffic.

**A large-scale view of web tracking and privacy.**

In this paper we report results from a January 2016 mea-







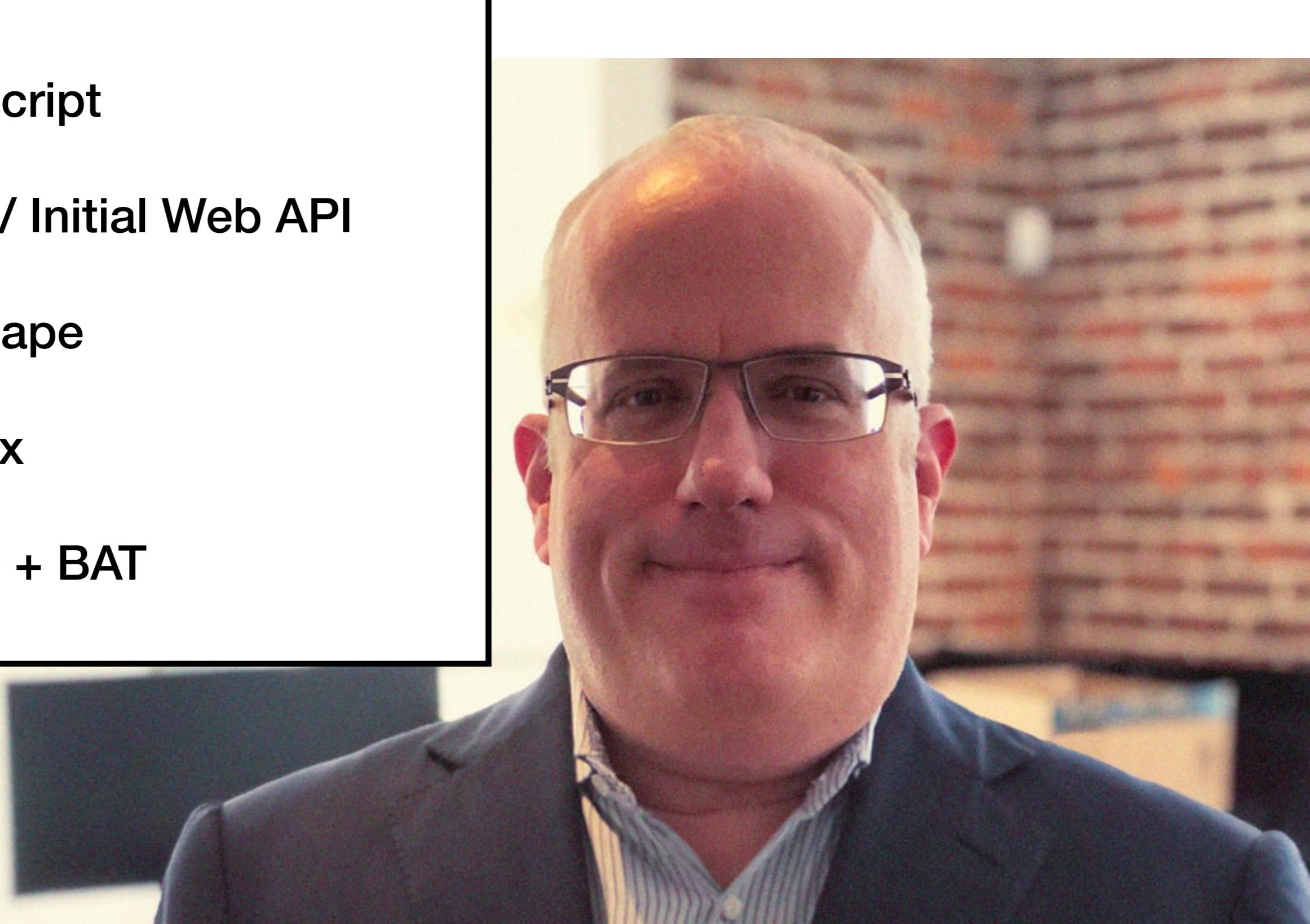
**But how much...  
a lot / too much**

# Overview

1. Why websites track
2. “Classic” tracking
3. Fingerprinting / “passive tracking”
4. Fingerprinting counter measures
5. Anti-finger printing exercise
6. Privacy protections in Brave
7. Wrapping up



- Javascript
- DOM / Initial Web API
- Netscape
- Firefox
- Brave + BAT



# Web 0.0

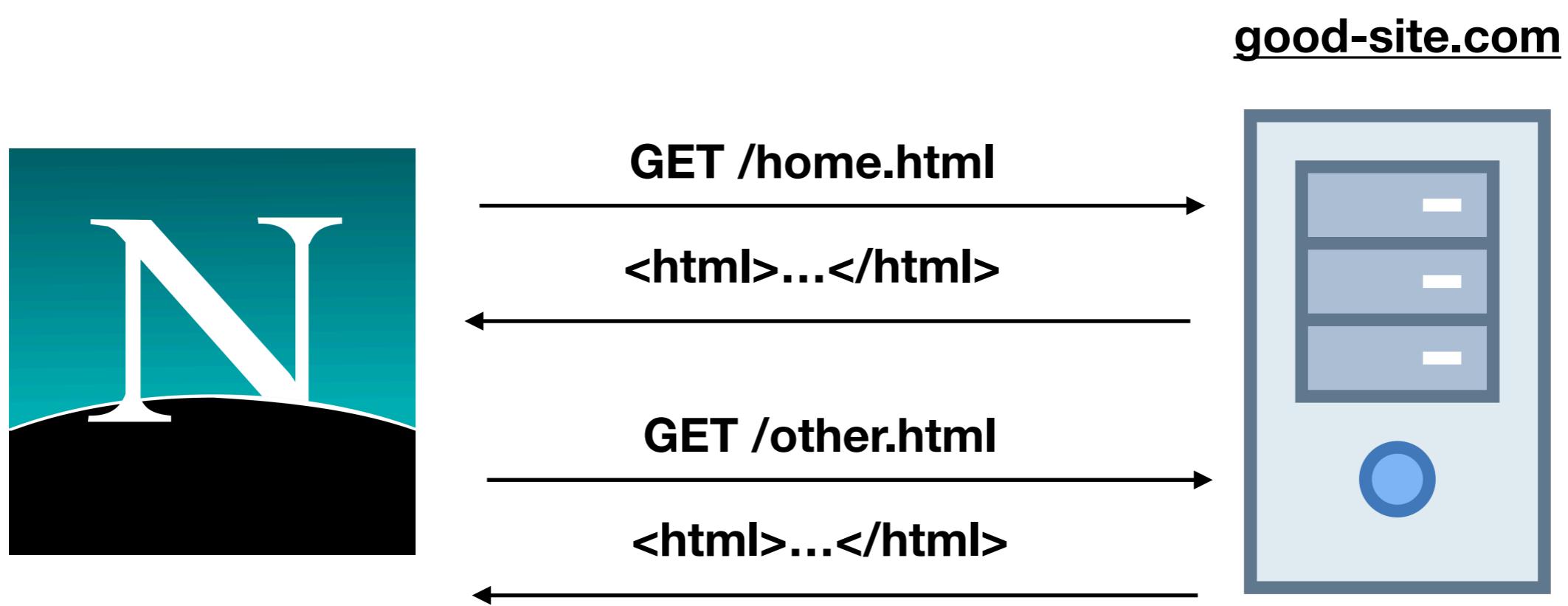
good-site.com



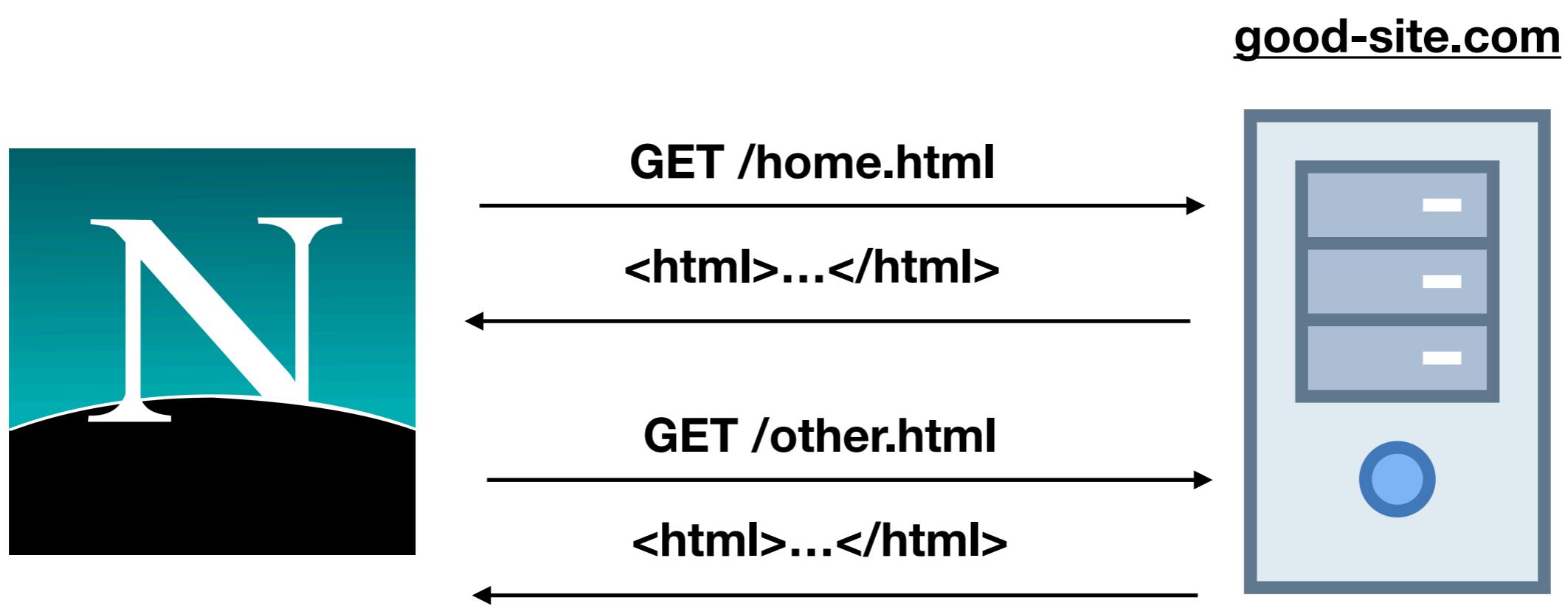
# Web 0.0



# Web 0.0



# Web 0.0



# Birth of the Tracking

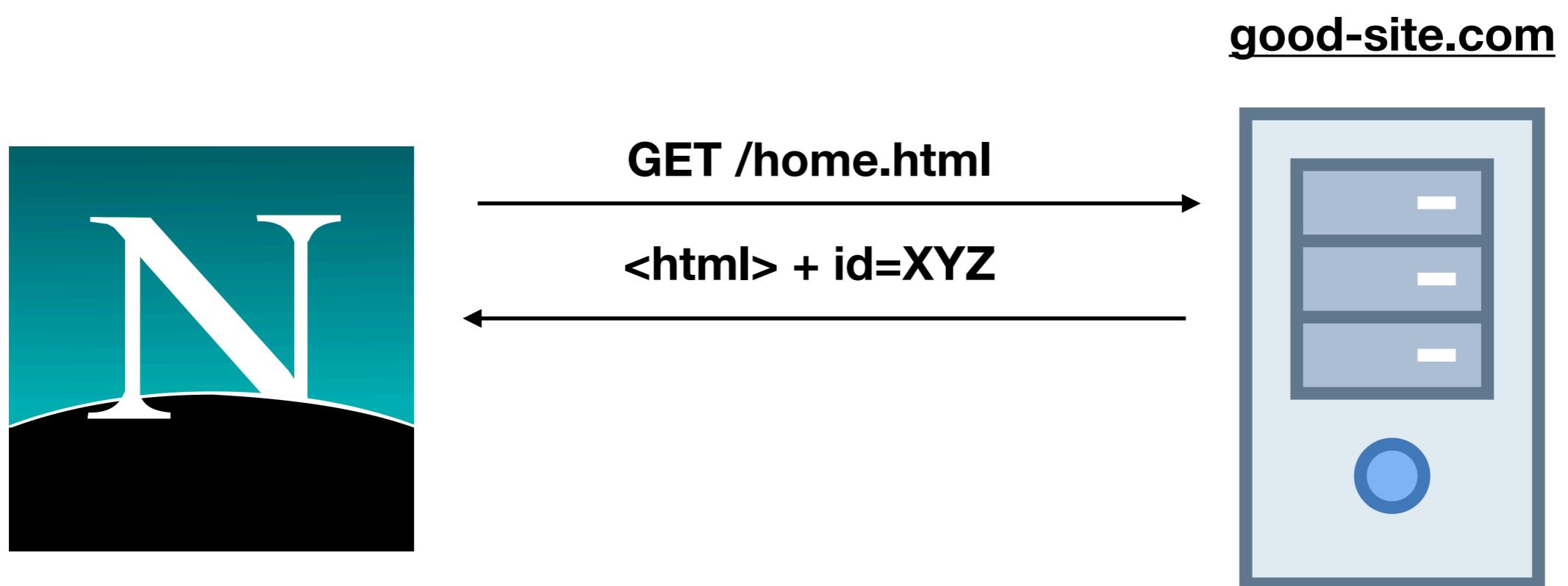
- **Problem**
  - Authentication?
  - Can't log in every time
  - HTTP auth is terrible and limited
- **Solution**
  - Server gives token to user
  - User returns it on requests
  - Aka “cookies”

# Web 0.0

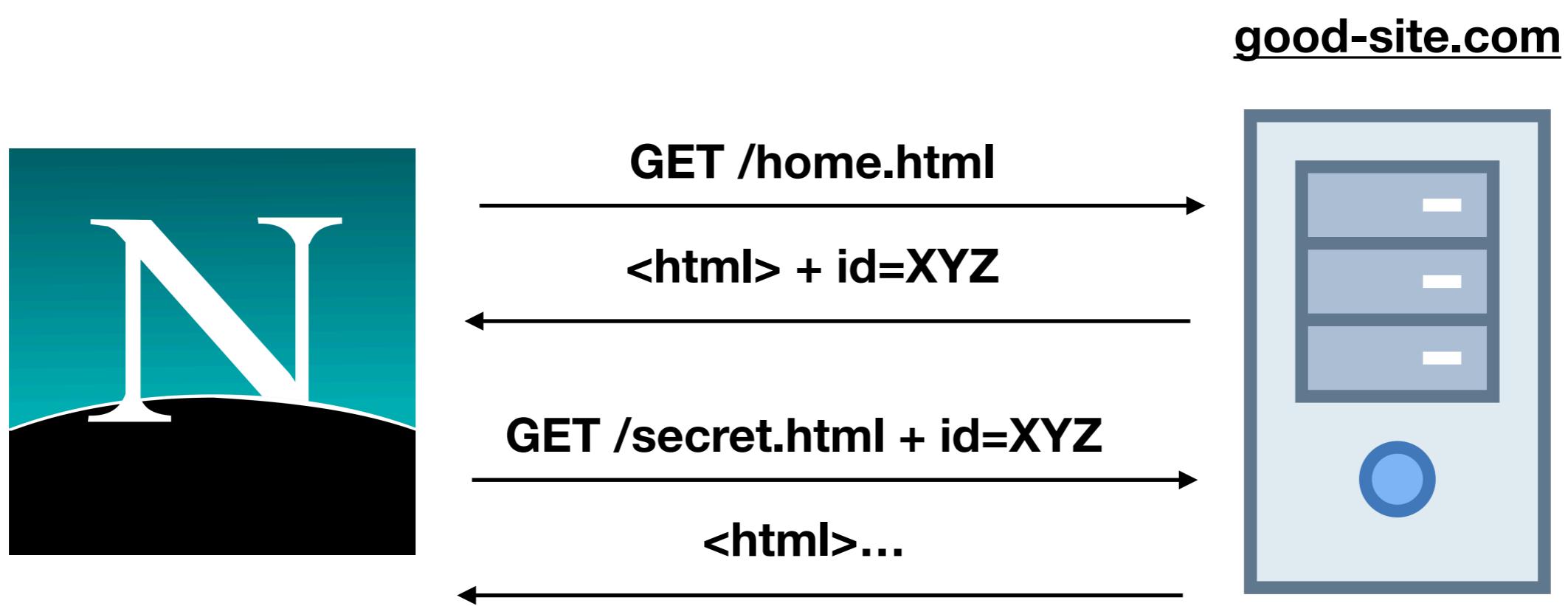
good-site.com



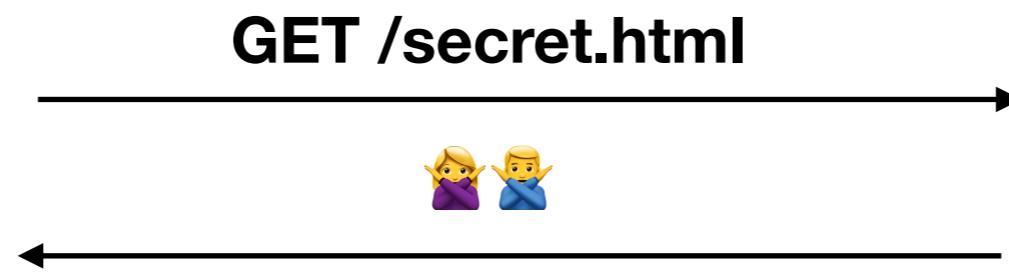
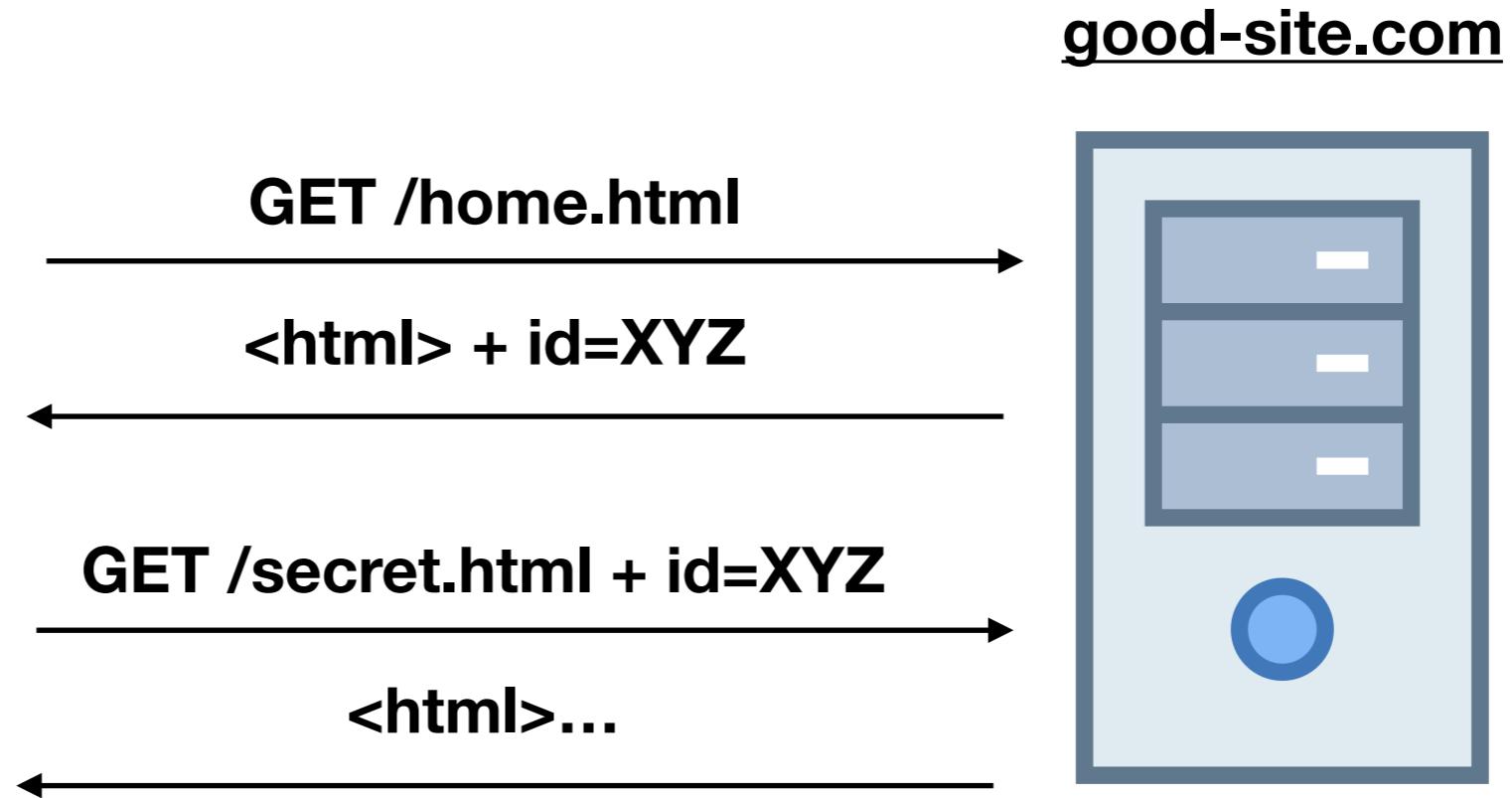
# Web 0.0



# Web 0.0



# Web 0.0



**But in the  
meantime...**

**cat-cuties.com**



**kozy-kittens.com**



**cat-cuties.com**



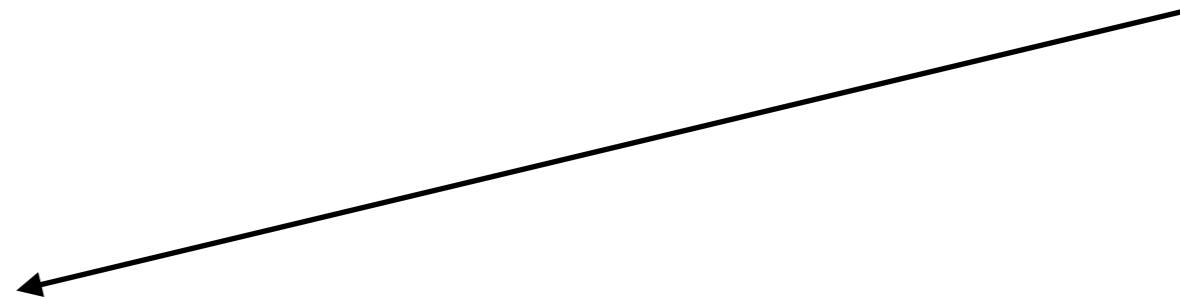
**kozy-kittens.com**



**cat-cuties.com**



**kozy-kittens.com**



**cat-cuties.com**



**kozy-kittens.com**

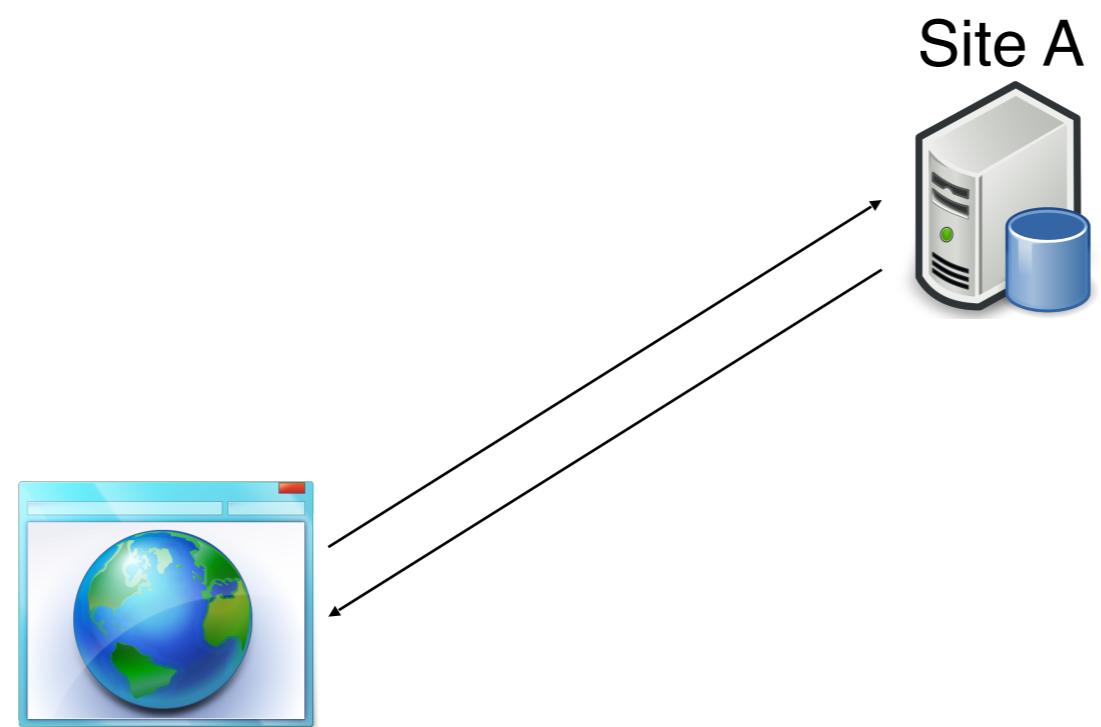


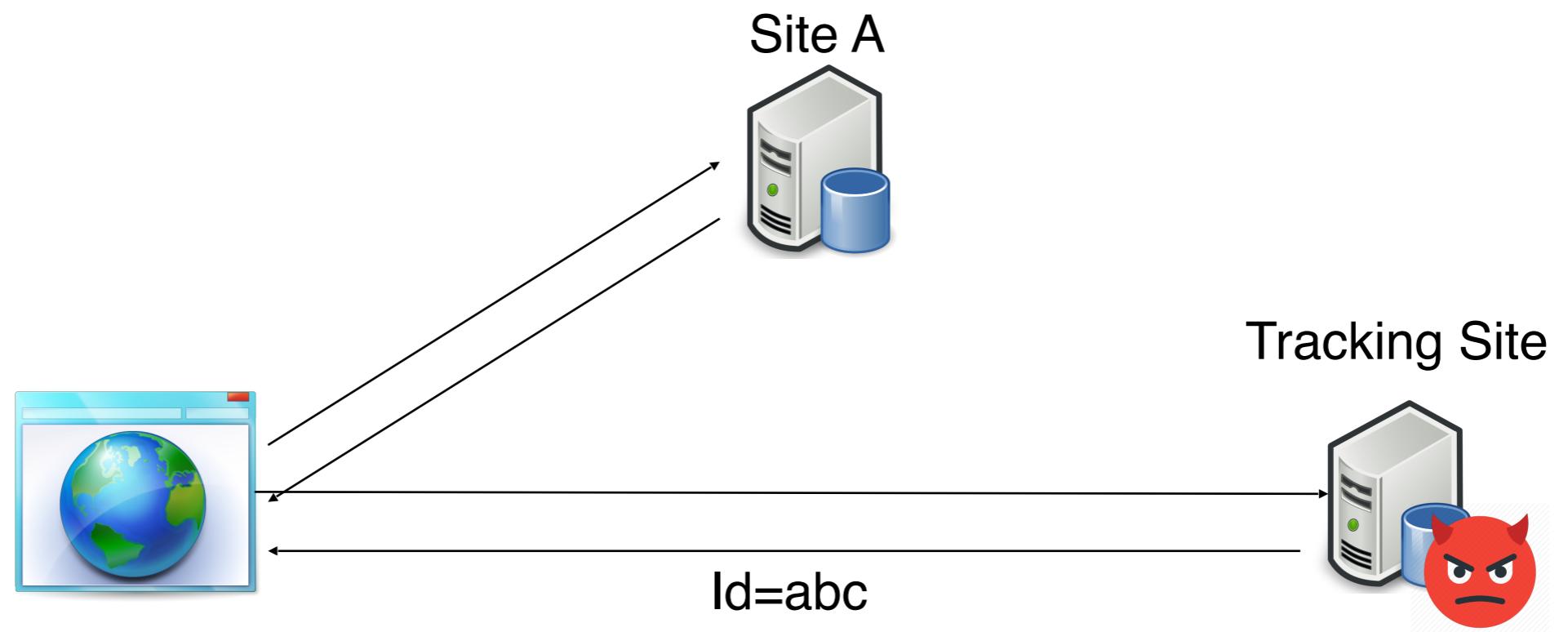
**cookies, cookies everywhere...**

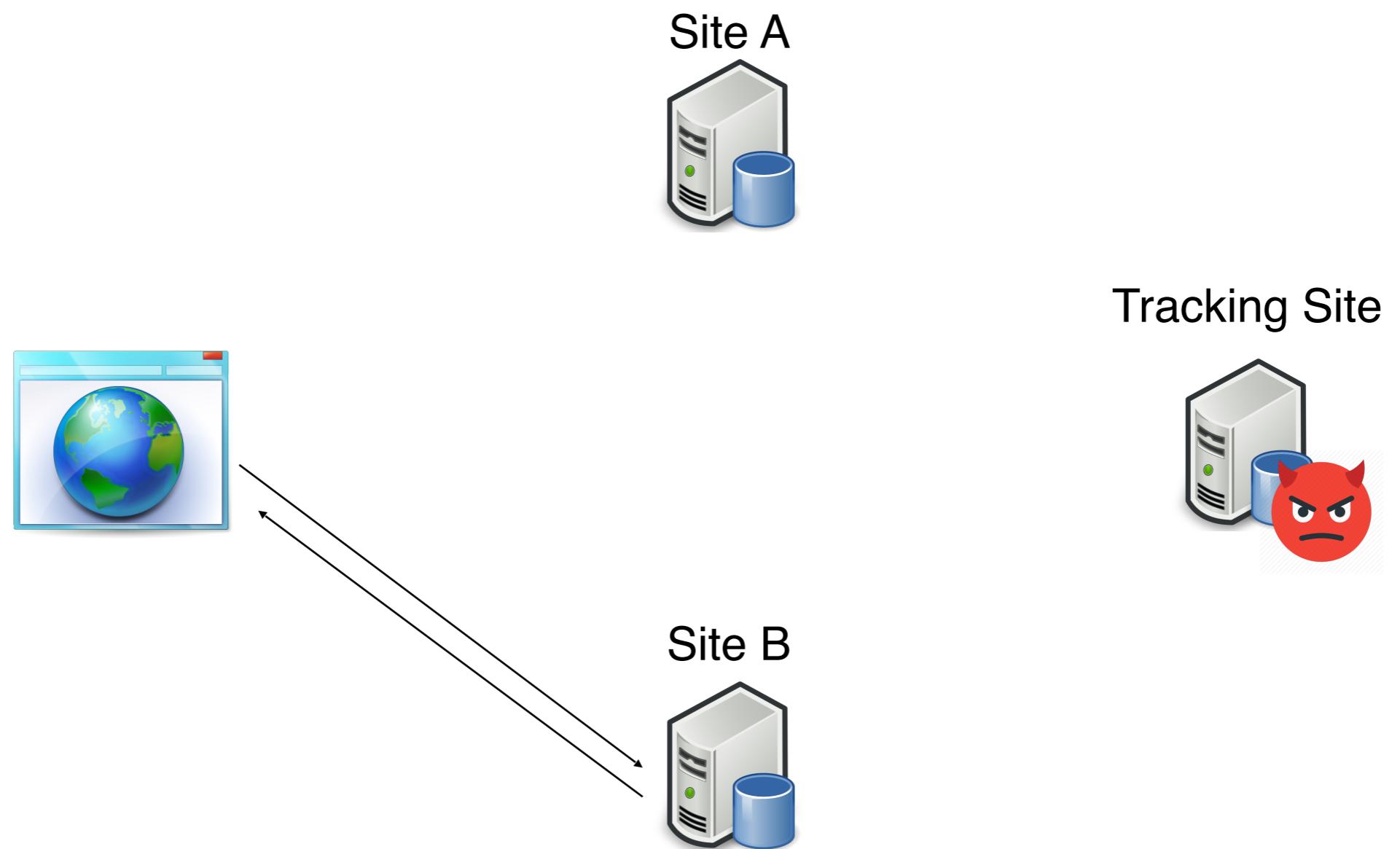
**Cookies  
+ 3p Resources**

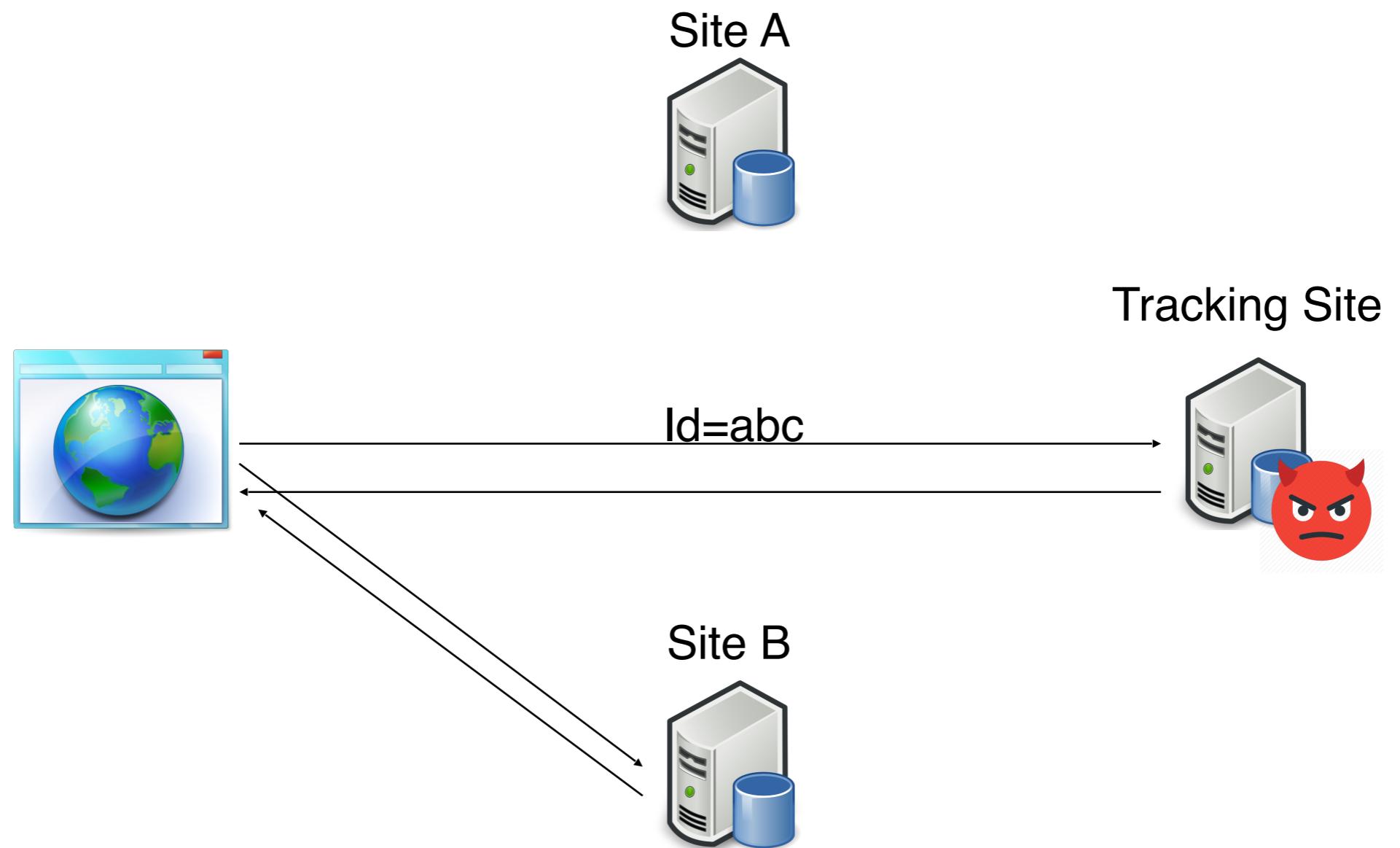
---

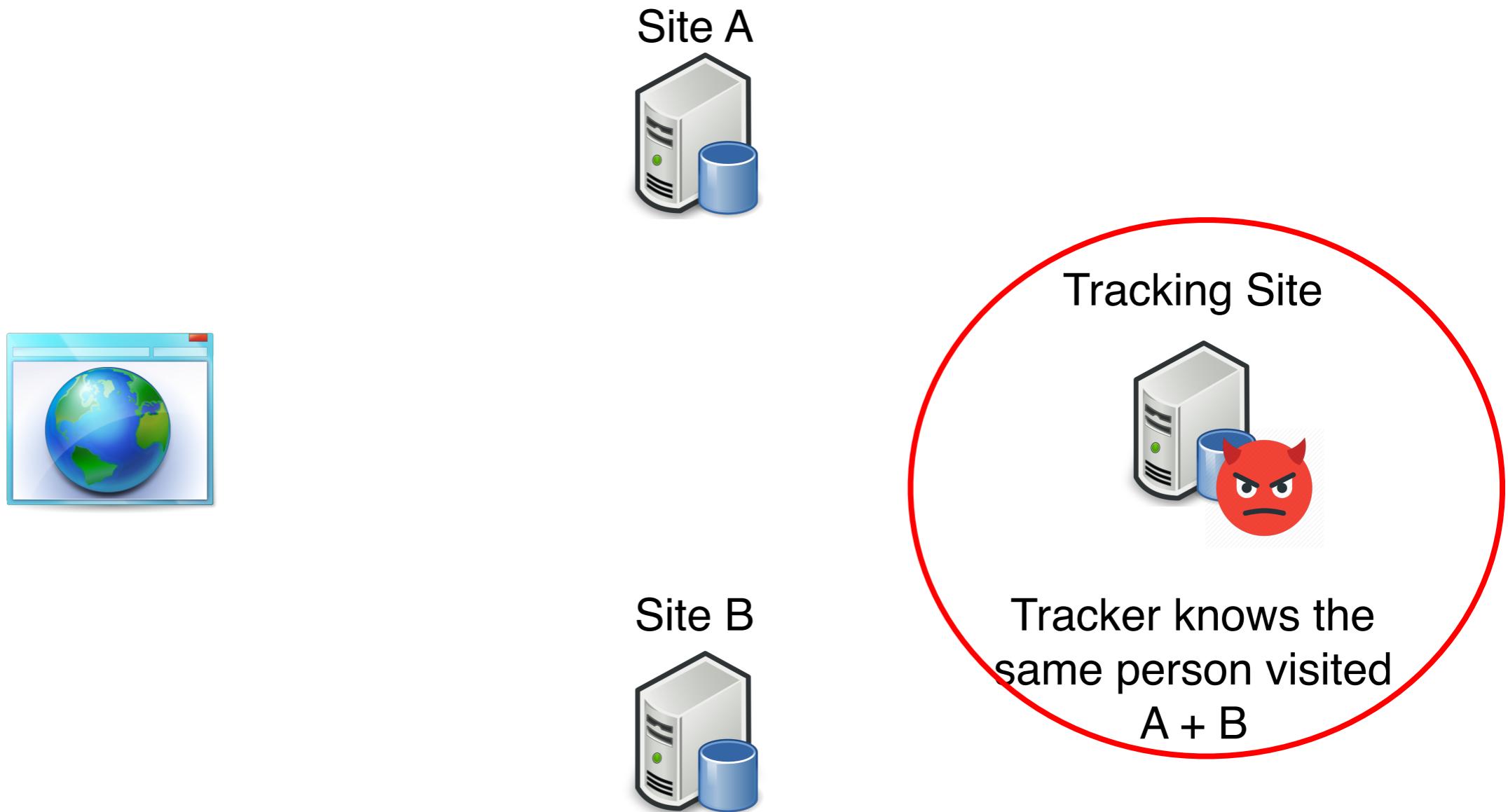
**Tracking**











# Tracking Patient Zero

- The internets “original sin”
  - cross origin resources
  - 3p cookies
  - or both...
- “I invitent Javascript and 3p script, and I’ve been making up for it ever sense...”  
(paraphrase)



# “Ever-Cookies”

- **Some browsers started fighting back**  
Brave, Safari, Firefox, extensions...
- **Trackers fought back**  
Moving IDs information out of cookies, to other location
- **Long list of locations**
  - Local and Session Storage
  - HSTS
  - Cache (etags, Cache API, etc)
  - Plugins
  - many many many more...

# Overview

1. Why websites track (and how much)
2. “Classic” tracking
- 3. Fingerprinting / “passive tracking”**
4. Fingerprinting in web standards
5. Fingerprinting counter measures
6. Anti-finger printing exercise
7. Wrapping up

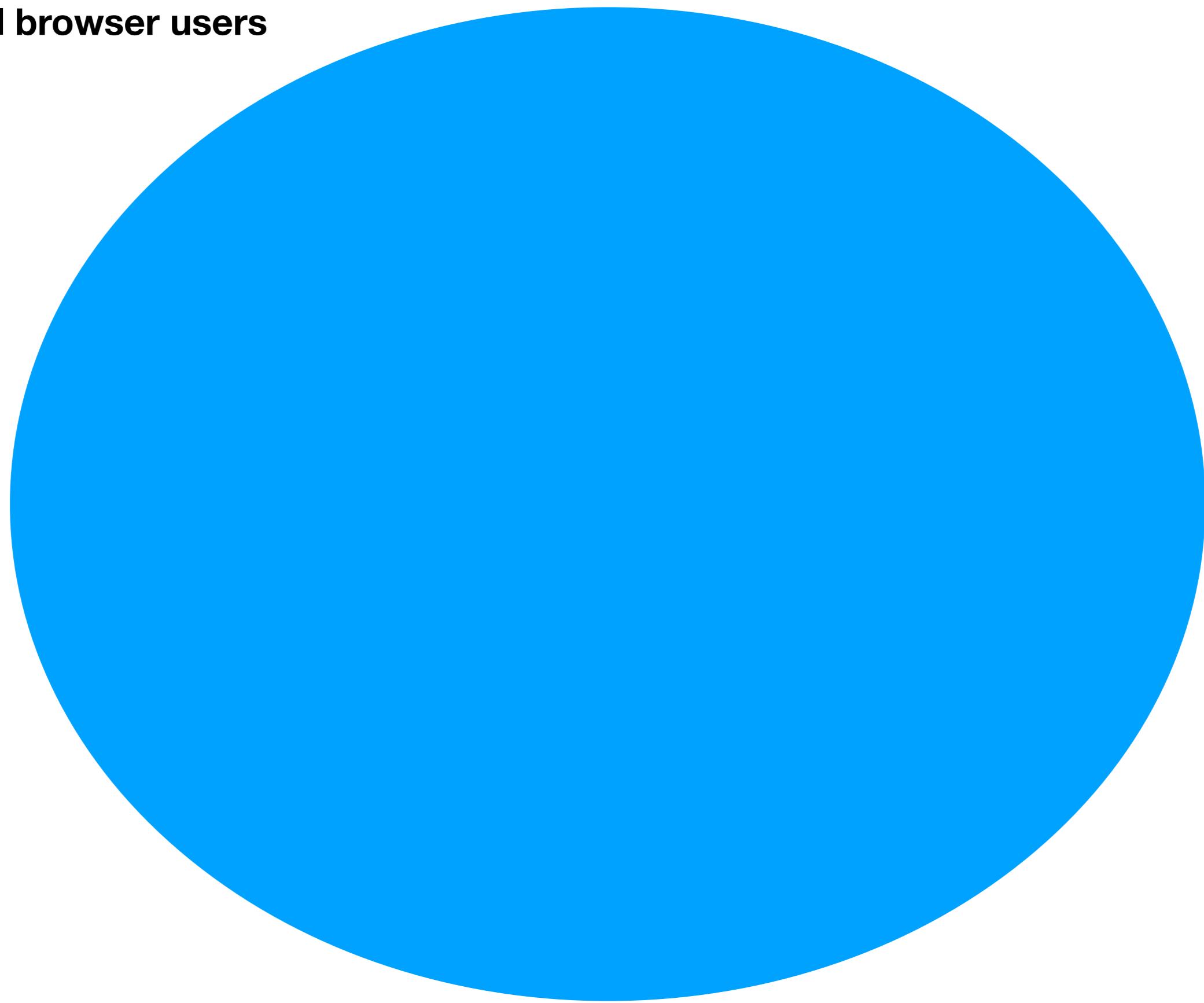
# Fingerprinting, what's diff?

- **Classic tracking**
  - Website stores an id on the client
  - The client returns the id to the server (cookie or JS)
  - The id is what allows re-identification
- **Fingerprinting / passive tracking**
  - Website finds things different about each visitor
  - That difference allows re-identification

# Fingerprinting, how

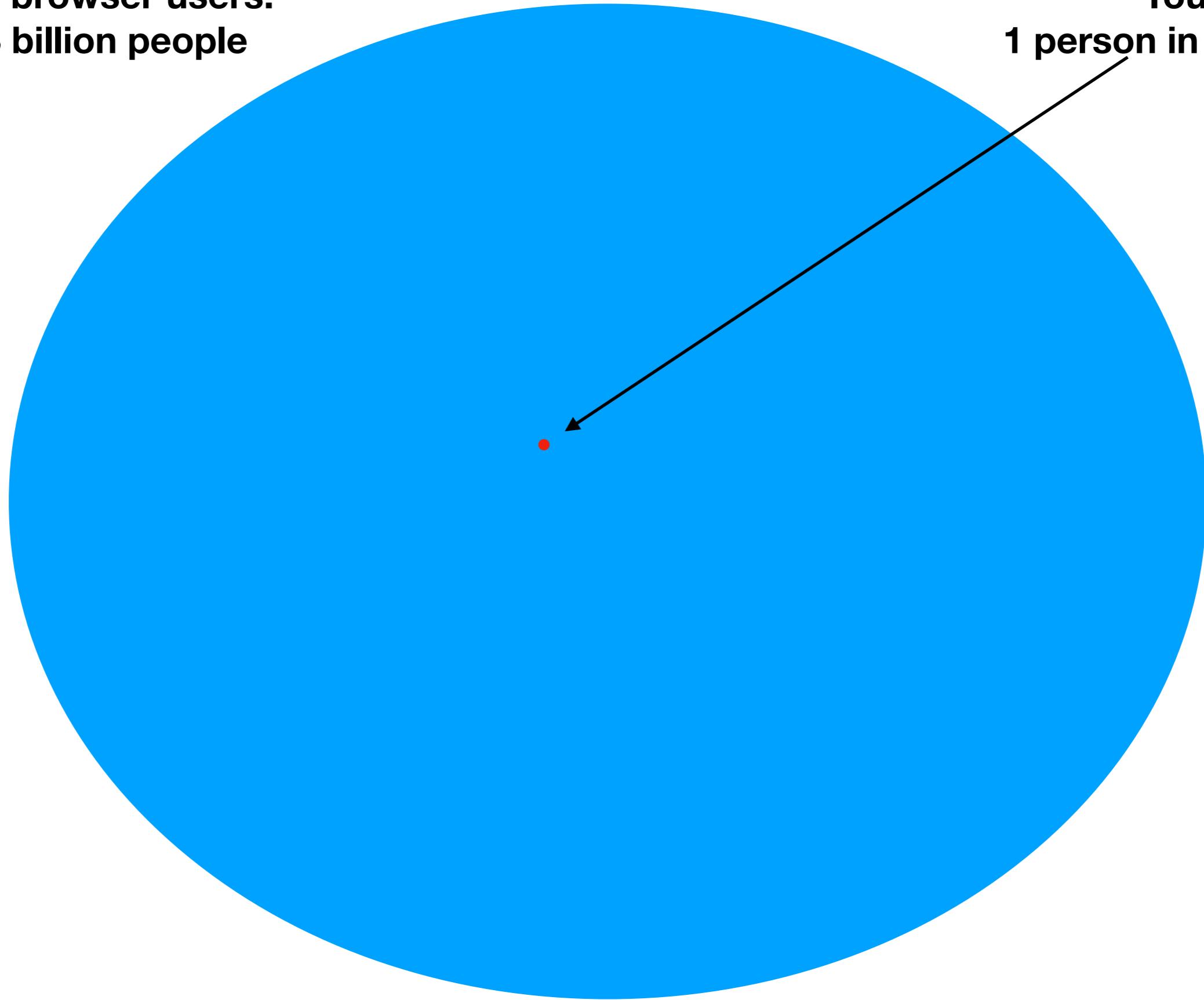
- Large number of semi-identifiers
  - Browser size
  - Extra fonts
  - Audio hardware
  - Video hardware
  - Installed plugins
  - Color depth
  - etc etc etc...

**All browser users**

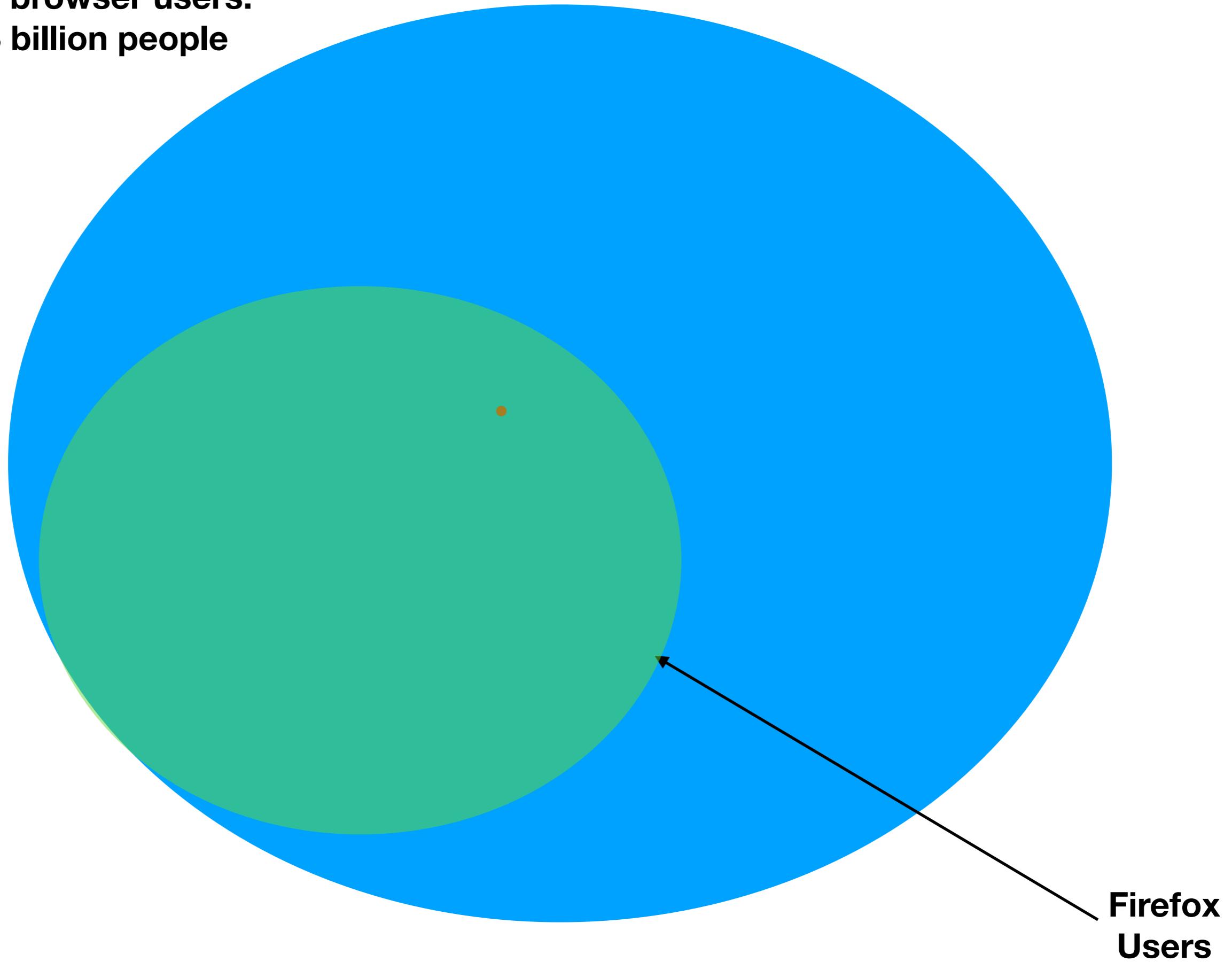


**All browser users:  
3 billion people**

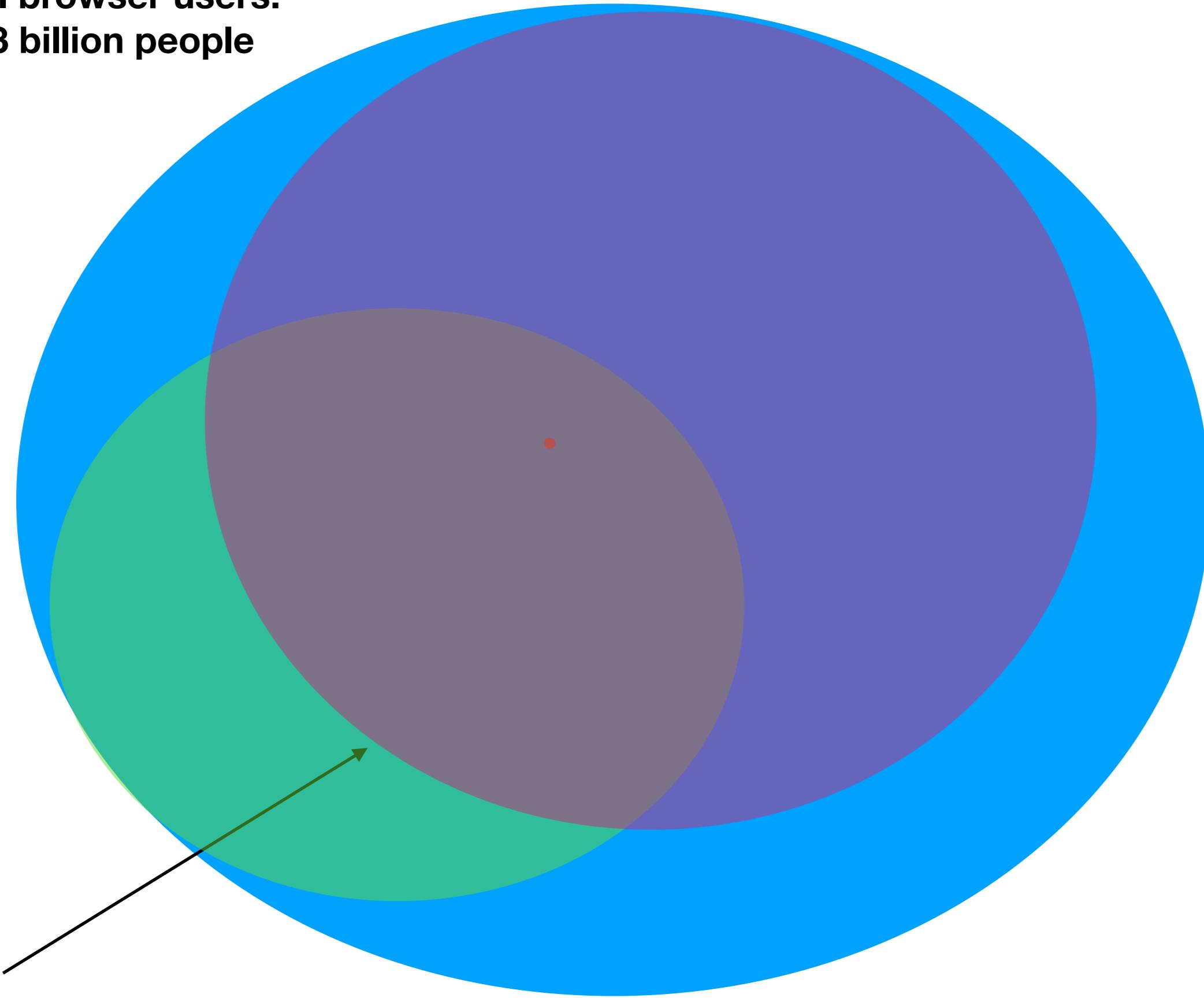
**You  
1 person in 3 billion**



**All browser users:  
3 billion people**



**All browser users:  
3 billion people**

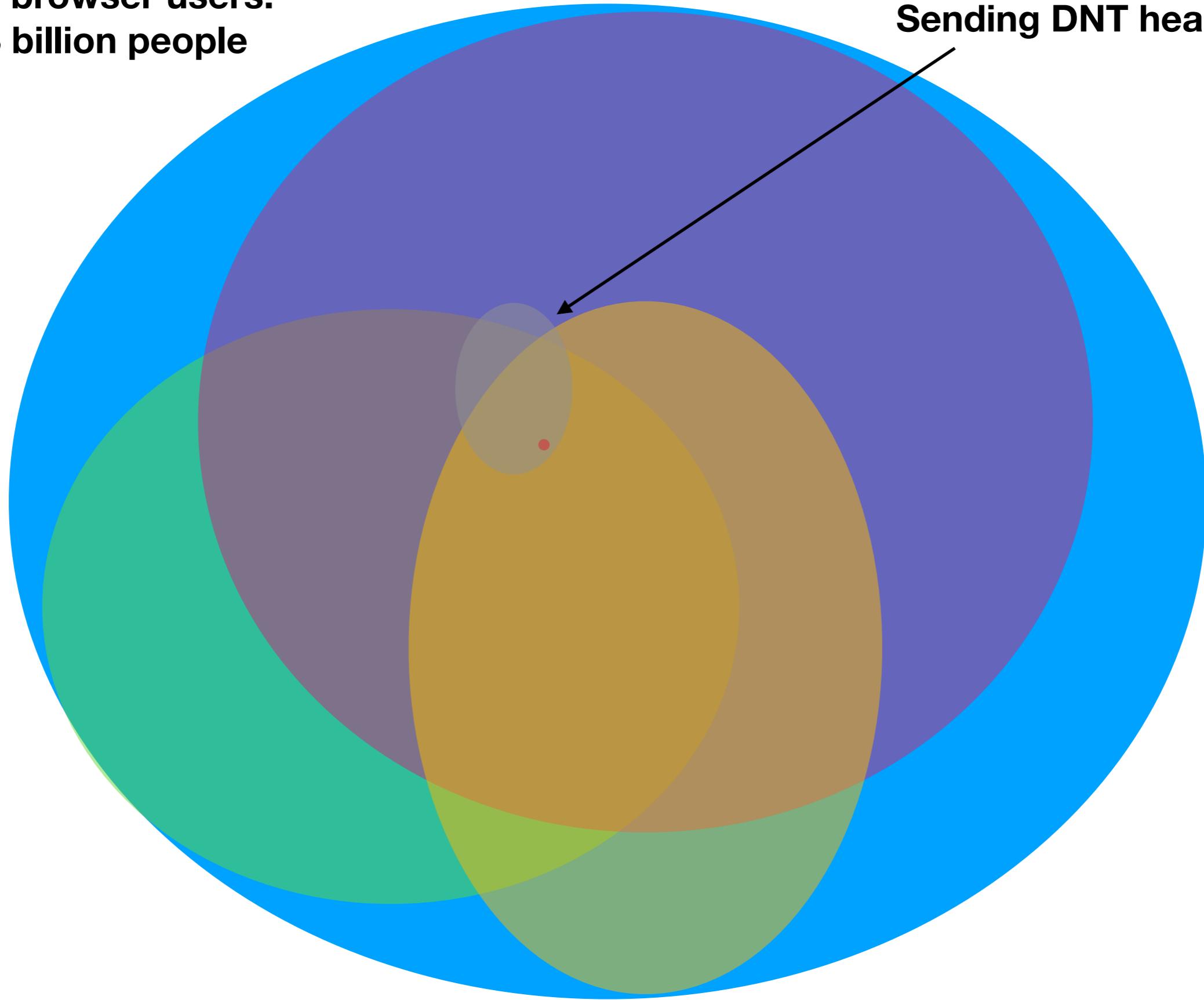


**Windows users**

**All browser users:  
3 billion people**

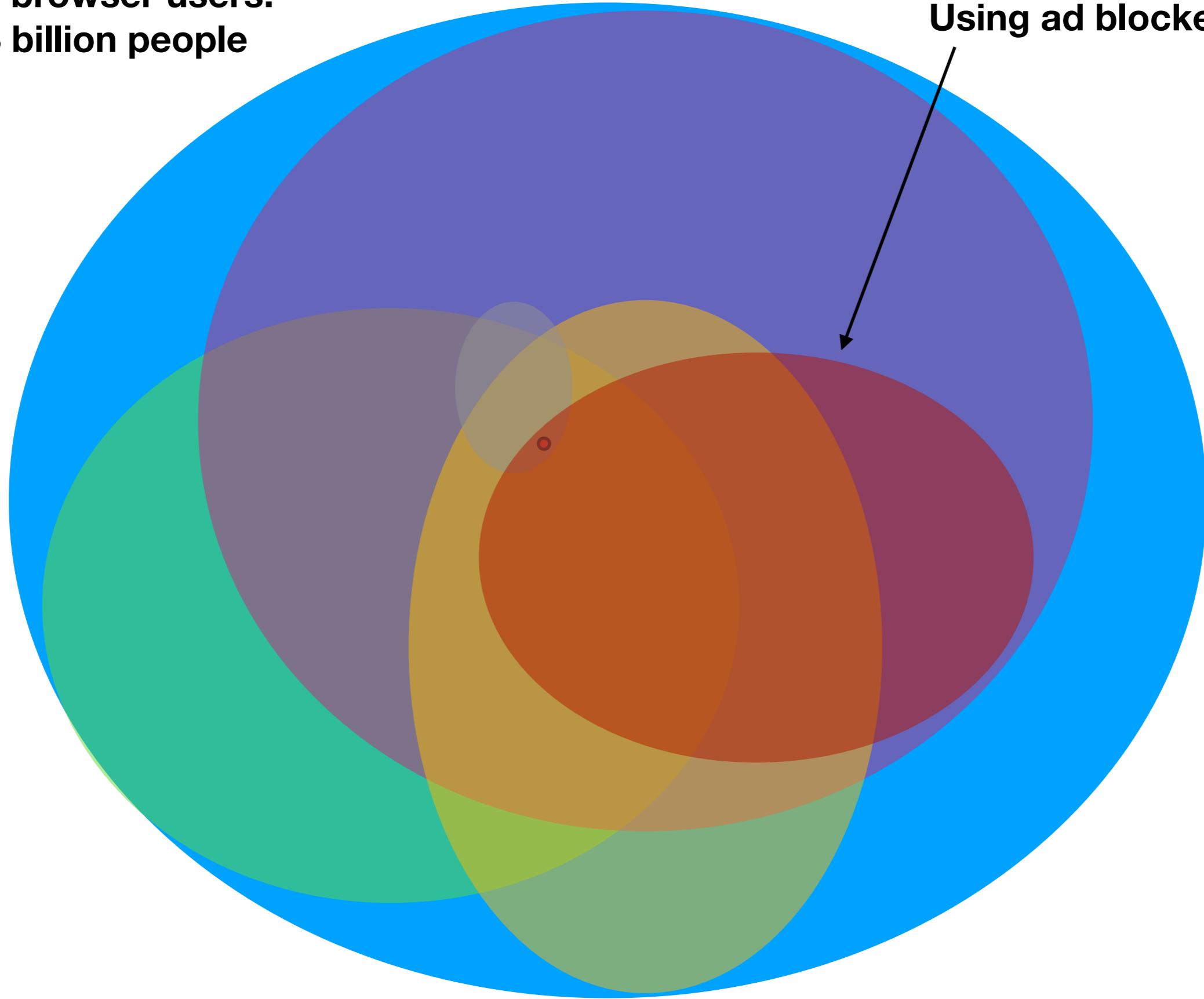


**All browser users:  
3 billion people**



**Sending DNT header**

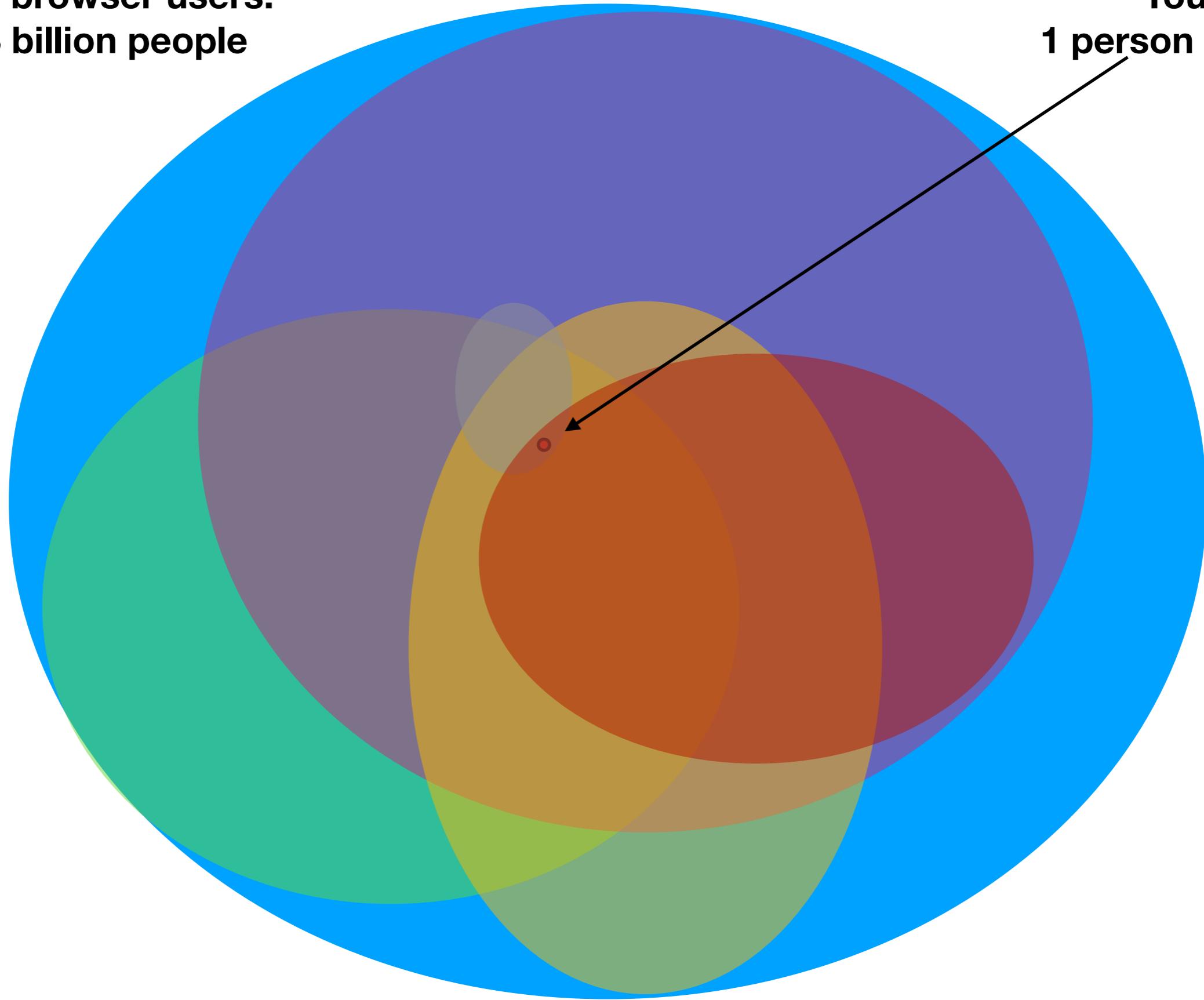
**All browser users:  
3 billion people**



**Using ad blocker**

**All browser users:**  
**3 billion people**

**You**  
**1 person in 100**



# Succeeding at Fingerprinting

## 1. Breath of fingerprints

Large number of semi-identifiers

## 2. Depth of fingerprints

How uniquely each identifier can... identify

# Breath (examples)

- User agent string
- Installed fonts
- Canvas / WebGL
- Hardware (many)
- Height / width

# User Agent String

- **History of the Browser user-agent string**  
<https://webaim.org/blog/user-agent-string-history/>
- **Katamari-Damacy of identifiers**
- **Brave / Chrome**  
Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.50 Safari/537.36
- **Easy to extract**
  - navigator.userAgent
  - User-Agent:

# Installed Fonts

- **Three categories of fonts**
  - System
  - Local
  - Web
- **“Local” is the tricky part**
  - Office
  - Photoshop
  - Goofery
- **Easy to extract**
  - plugins
  - css + span + width

**[‘Andale Mono’, ‘Arial’, ‘Arial Black’, ‘Arial Hebrew’,  
‘Arial MT’, ‘Arial Narrow’, ‘Arial Rounded MT Bold’...]**

**[‘Andale Mono’, ‘Arial’, ‘Arial Black’, ‘Arial Hebrew’,  
‘Arial MT’, ‘Arial Narrow’, ‘Arial Rounded MT Bold’...]**

<span>Example</span>

**[‘Andale Mono’, ‘Arial’, ‘Arial Black’, ‘Arial Hebrew’,  
‘Arial MT’, ‘Arial Narrow’, ‘Arial Rounded MT Bold’...]**

**For each font...**



**<span>Example</span>**

**[‘Andale Mono’, ‘Arial’, ‘Arial Black’, ‘Arial Hebrew’,  
‘Arial MT’, ‘Arial Narrow’, ‘Arial Rounded MT Bold’...]**

**For each font...**

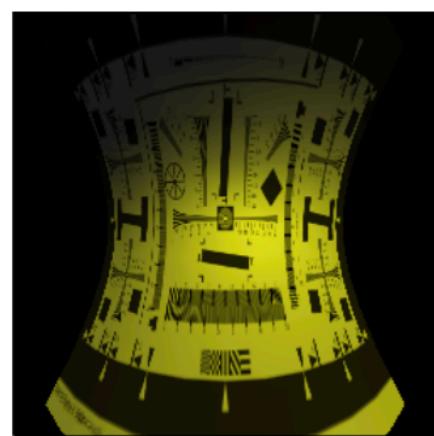
**Fingerprinter**

```
for (const fontName of fonts) {  
    // 1. Apply font to span  
    // 2. Measure width of span  
    // 3. If it changes, user has font...  
}
```

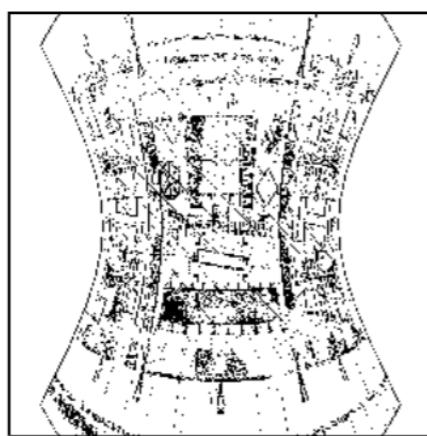
`<span>Example</span>`

# Canvas / WebGL

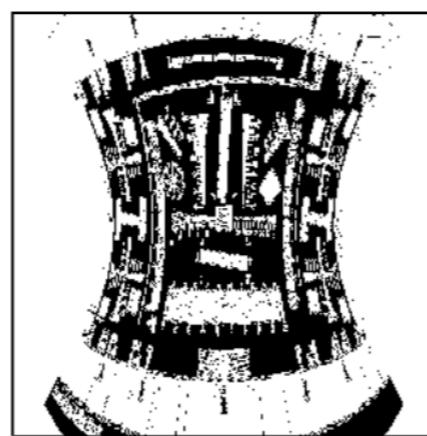
- **Pixel Perfect: Fingerprinting Canvas in HTML5**  
Keaton Mowery and Hovav Shacham
- **Drawing APIs**  
e.g. Drawing lines / shapes
- **Standardized, but subtle differences**
- **Easy to extract**
  - Create canvas
  - Do some drawing
  - toDataURL()



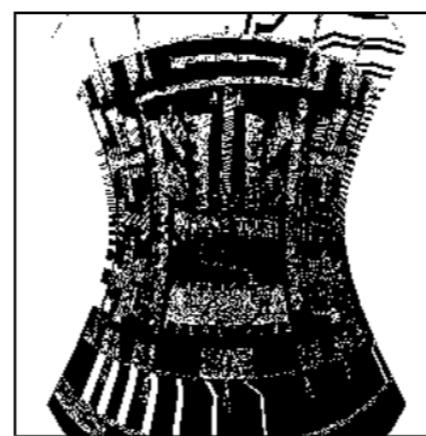
(a) Original  
(Intel G41)



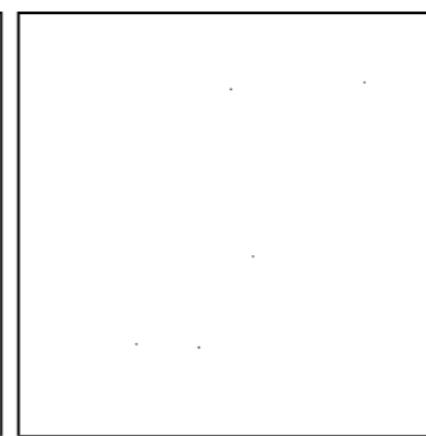
(b) Group 1  
(Radeon HD 2400)



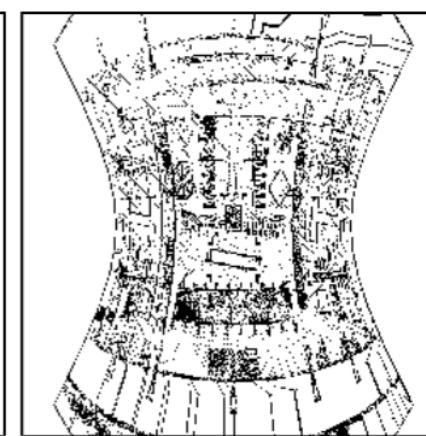
(c) Group 20  
(Intel 82945G)



(d) Group 23  
(Intel G33/G31)



(e) Group 25  
(Intel HD Graphics)



(f) Group 36  
(GeForce 6200)



## **Hovav Shacham**

**The Geometry of Innocent Flesh on the Bone:  
Return-into-libc without Function Calls**

# Hardware Identifiers

- **Many Web APIs leak capabilities**
  - number of cores (HTML)
  - number of audio channels (Web Audio API)
  - num shaders and similar (WebGL API)
  - device memory (Device Memory API)
  - network (WebRTC, Network status API)
- **Semi identifying**
- **Easy to extract**
  - All browsers have subset of the above
  - Most platforms have no permissions

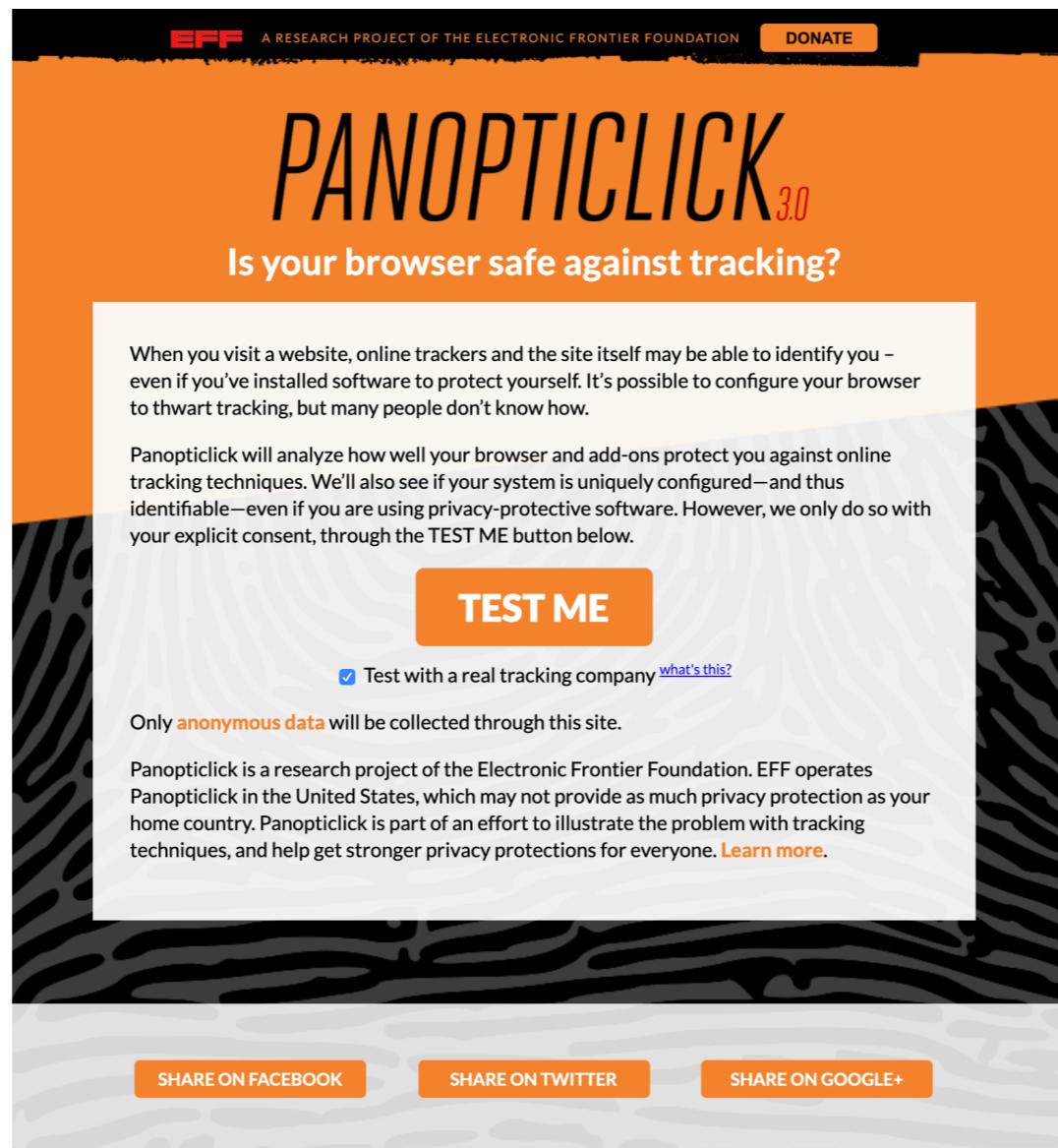
# Height / Width



# **Height / Width**

- **What does it mean?**
- **How to extract w/ JavaScript?**
- **How to extract w/o JavaScript?**
- **Brb 5 min (Go go go go go!)**

# Fingerprinting Depth



<https://panopticlick.eff.org/>

# Fingerprinting in Practice

- Needs to be in a database...
- Hash each endpoint
- Hash each value into a single identifier...
- Nice implication: “poisionability”...

# Exercise

- Read `fingerprint2.js`
- List as many finger-printing approaches as possible
- Understand how they're carried out
- Predict which are most identifying

# Overview

1. Why websites track (and how much)

2. “Classic” tracking

3. Fingerprinting / “passive tracking”

**4. Fingerprinting counter measures**

5. Anti-finger printing exercise

6. Privacy protections in Brave

7. Wrapping up

# Fingerprinting Countermeasures

- Remove the functionality
- Make the functionality consistent
- Restrict access (permissions, 1p vs 3p, user gesture, etc)
- Noise
- “Privacy budget”

# Remove the functionality

- Delete JS end point
- Remove the HTTP header
- Remove the runtime capability

# Consistency

- Make every browser return the same value
- ... or, most?
- Not that diff in practice from “removing”

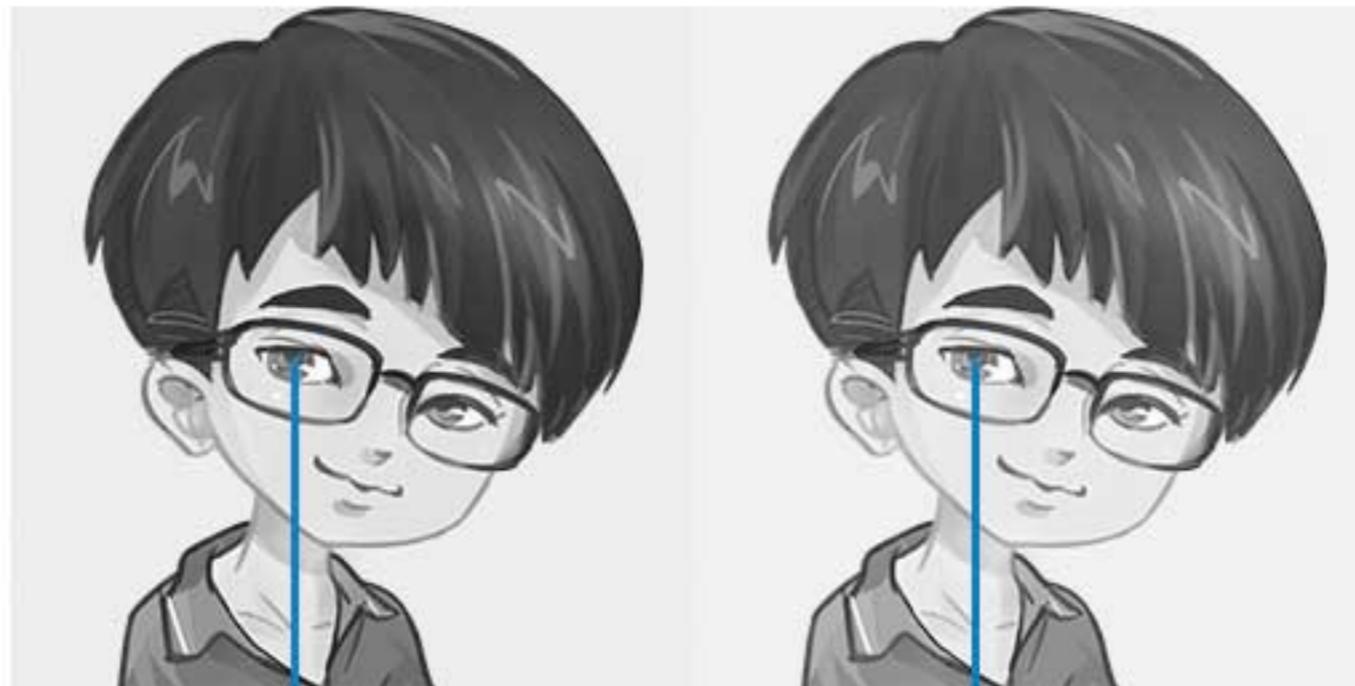
# Restrict access

- Permission prompt
- User gesture
- 1p vs. 3p
- “Site engagement”

# Noise

- Stenography
- Make different every time

Original   With Hidden Data



00110101

00110100

# Privacy Budget

- Allow some identifiability
- After “identifiability budget” is exhausted do... something
- Google folks love it
- Everyone else is... skeptical

# Overview

1. Why websites track (and how much)
2. “Classic” tracking
3. Fingerprinting / “passive tracking”
4. Fingerprinting counter measures
- 5. Anti-finger printing exercise**
6. Privacy protections in Brave
7. Wrapping up

# Fingerprint2 Again...

- Choose two fingerprinting vectors to combat
  - Propose counter measures
- Choose two fingerprinting vectors that are hard
  - Why are counter measures hard?

# Fingerprint2 pt 3...

- Pretend you the attacker
- How would you respond to those defenses...

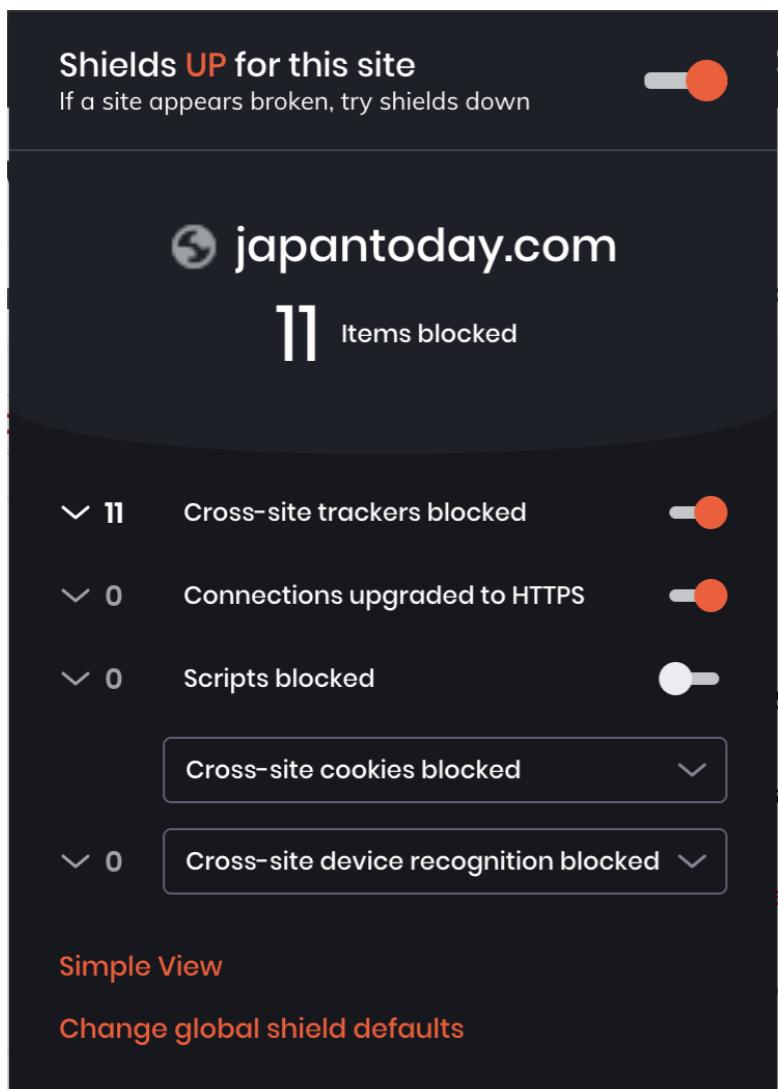
# Fingerprint2 pt 4...

- Pretend you the defender again
- How would you modify your defenses given the previous round...

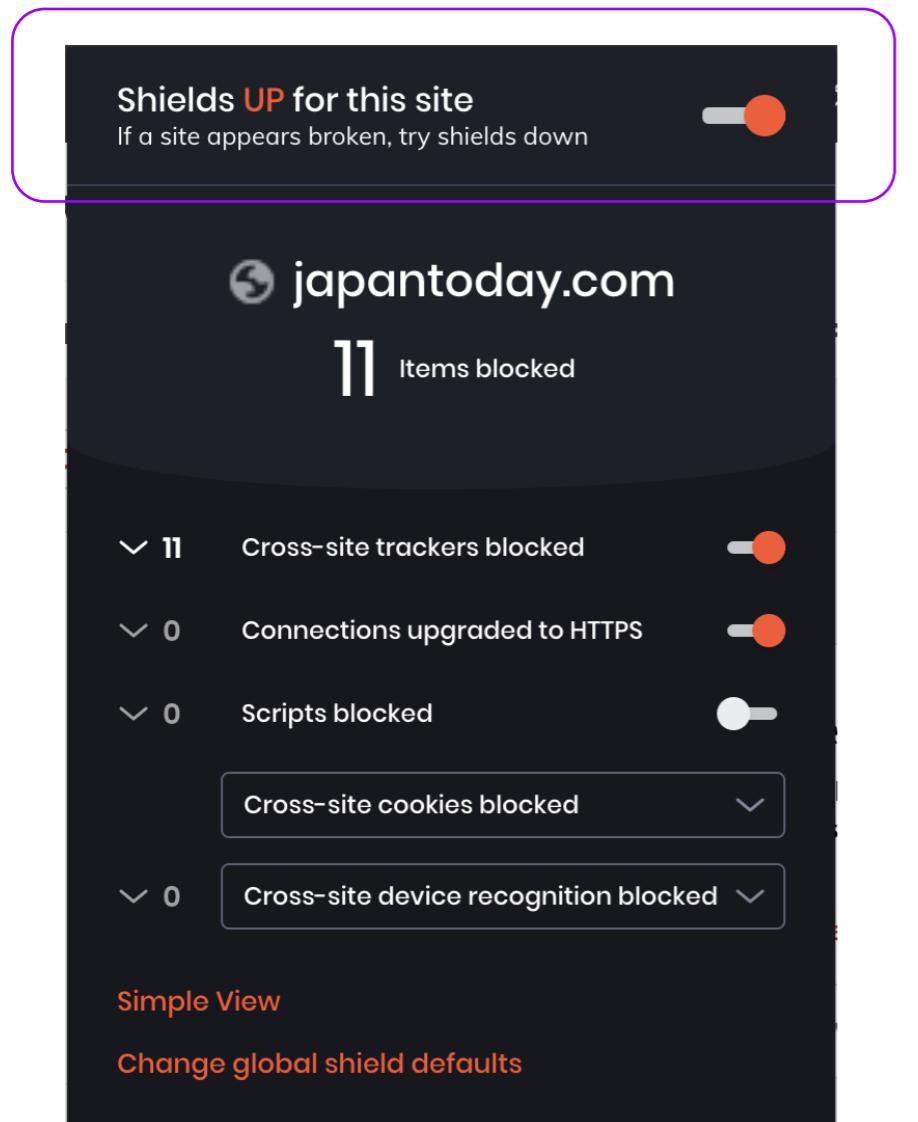
# Overview

1. Why websites track (and how much)
2. “Classic” tracking
3. Fingerprinting / “passive tracking”
4. Fingerprinting counter measures
5. Anti-finger printing exercise
6. **Privacy protections in Brave**
7. Wrapping up

# Brave Privacy Protections

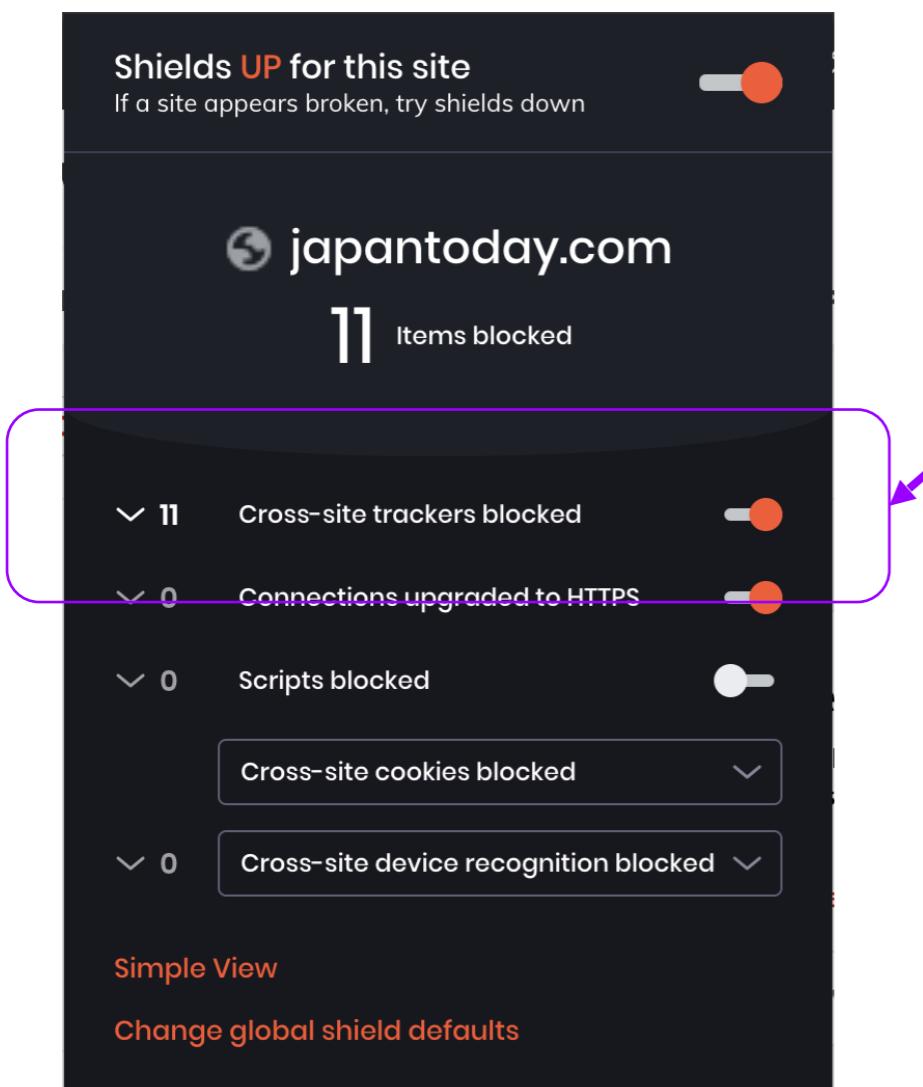


# Brave Privacy Protections



- Shields
- Global protection from tracking
- On by default
- Can be disabled if needed

# Brave Privacy Protections



- Block cross site trackers
- Lists of known tracking websites
- Refuse to load
- Both community and Brave generated

# **Blocking Cross-Site Trackers in Brave**

---

- **EasyList and EasyPrivacy**

Used by AdBlock Plus, etc.

- **Disconnect**

Used by Firefox, extensions

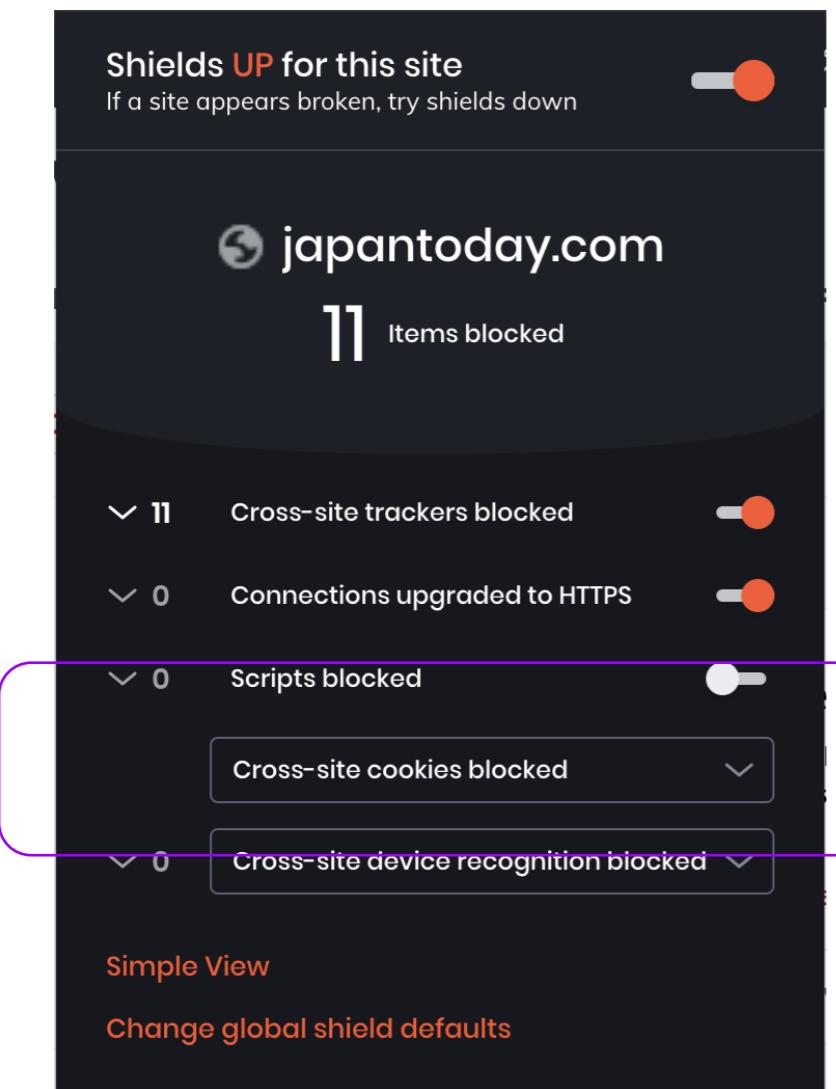
- **uBlock Origin**

Excellent blocking extension

- **Brave generated**

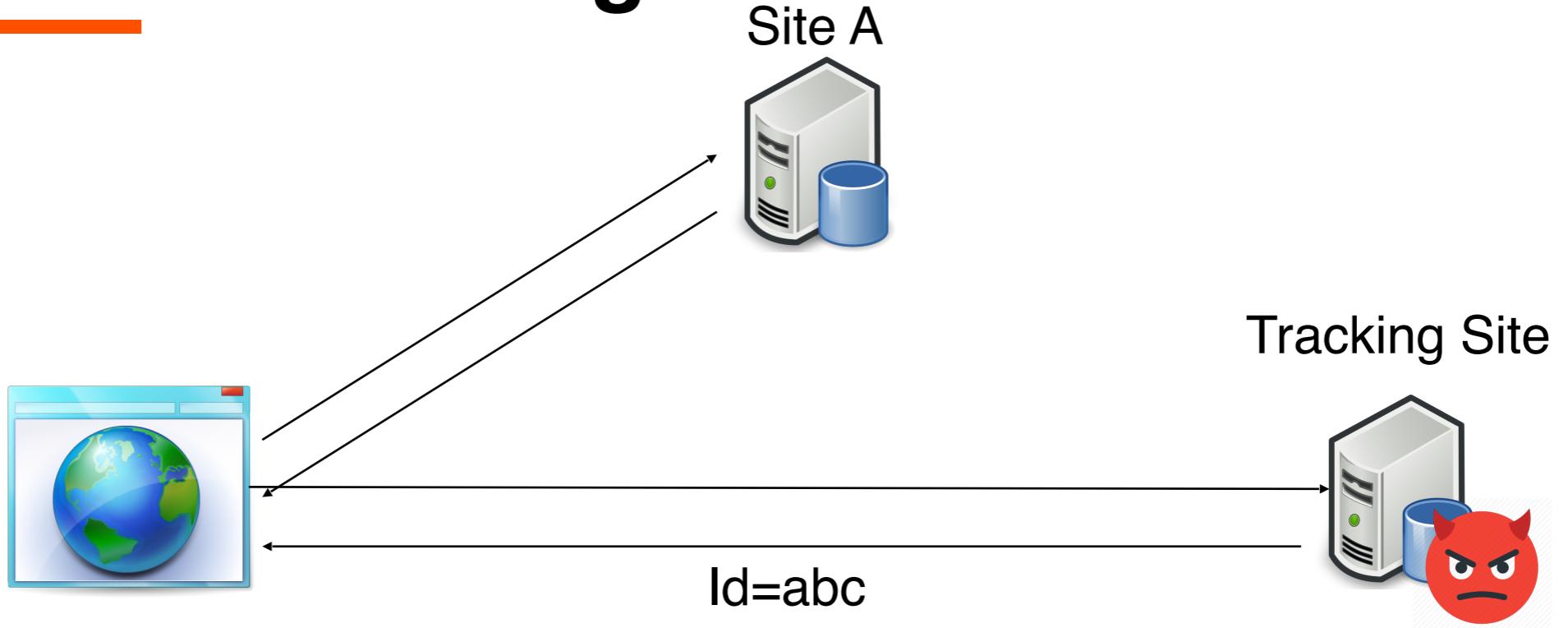
Open source, shared with  
community

# Brave Privacy Protections

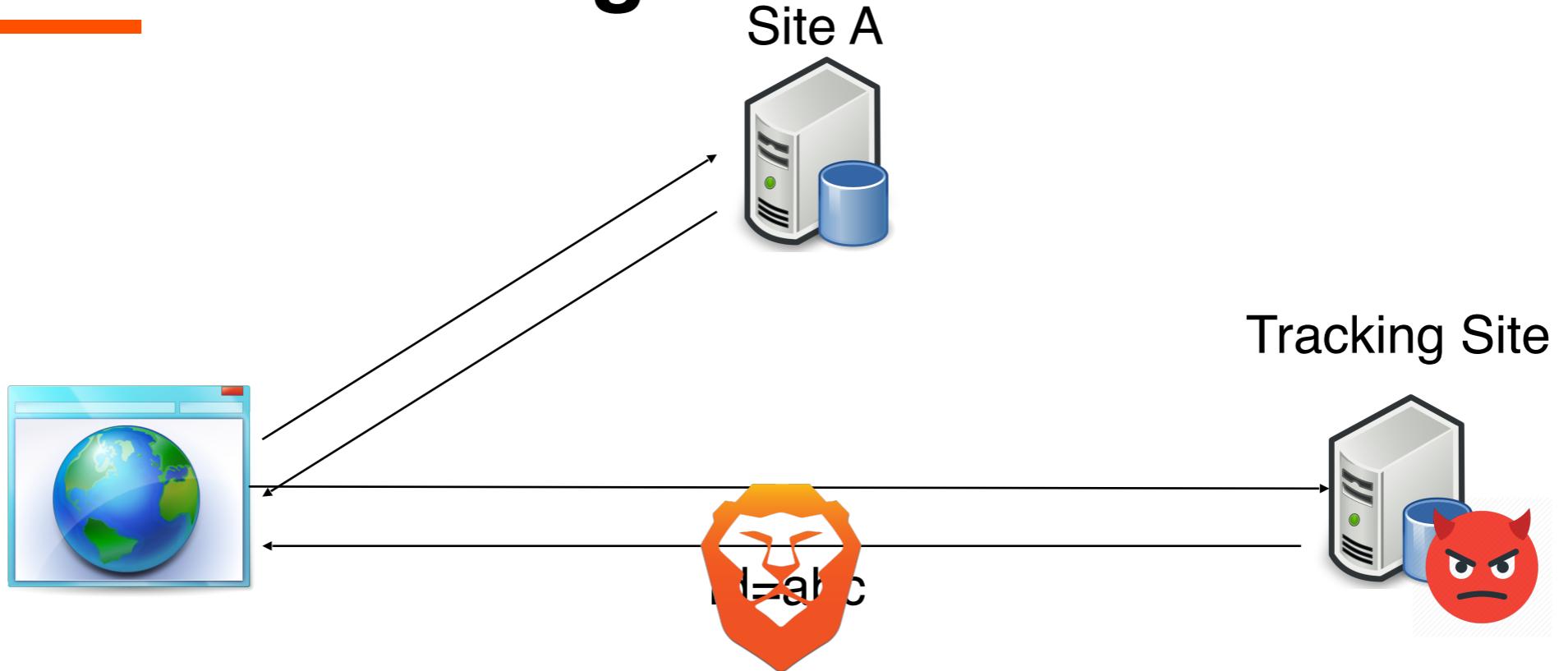


- Don't send identifiers to third party sites
- Send to “main” site
- Same with other storage methods

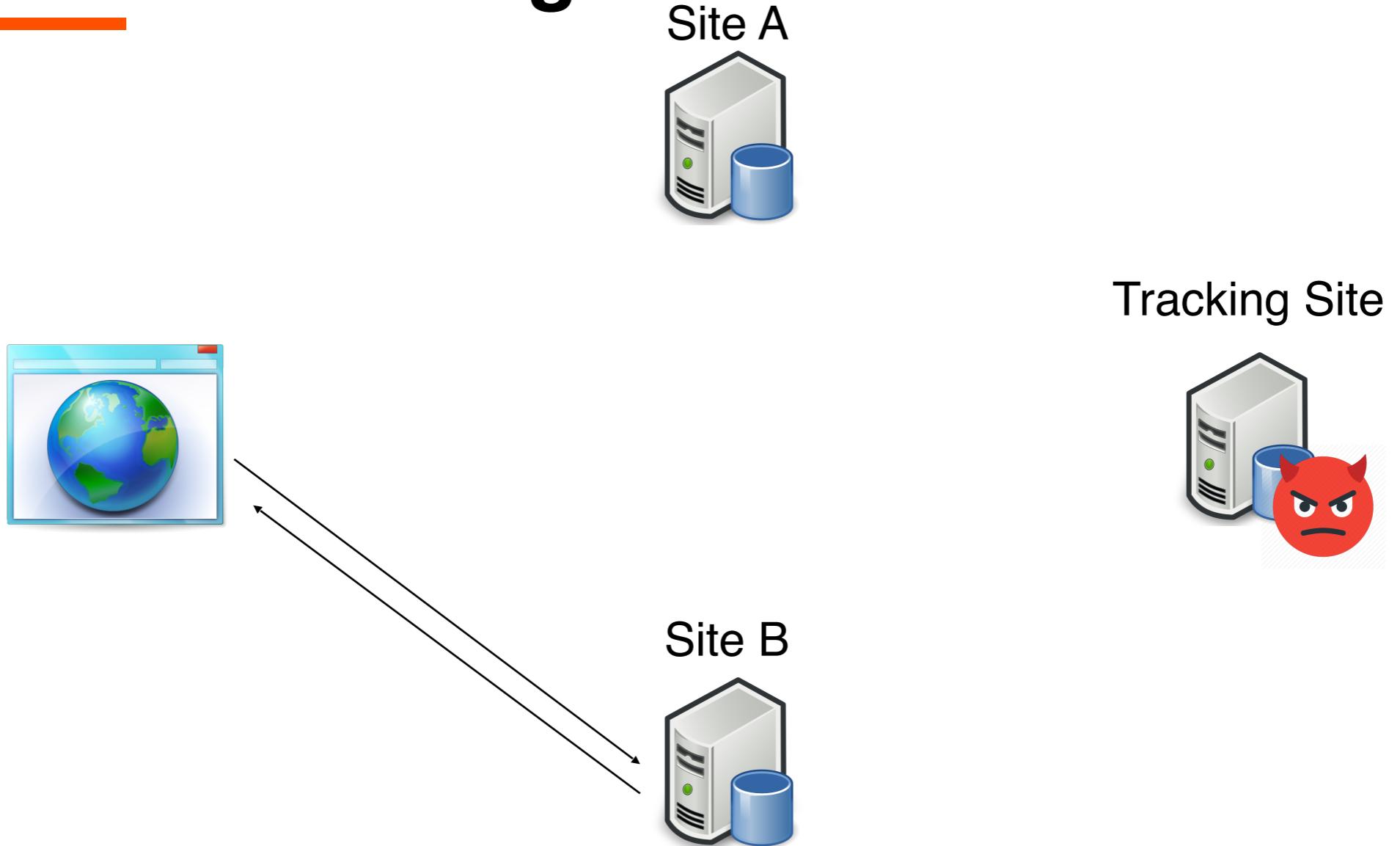
# Brave Blocks Tracking Cookies



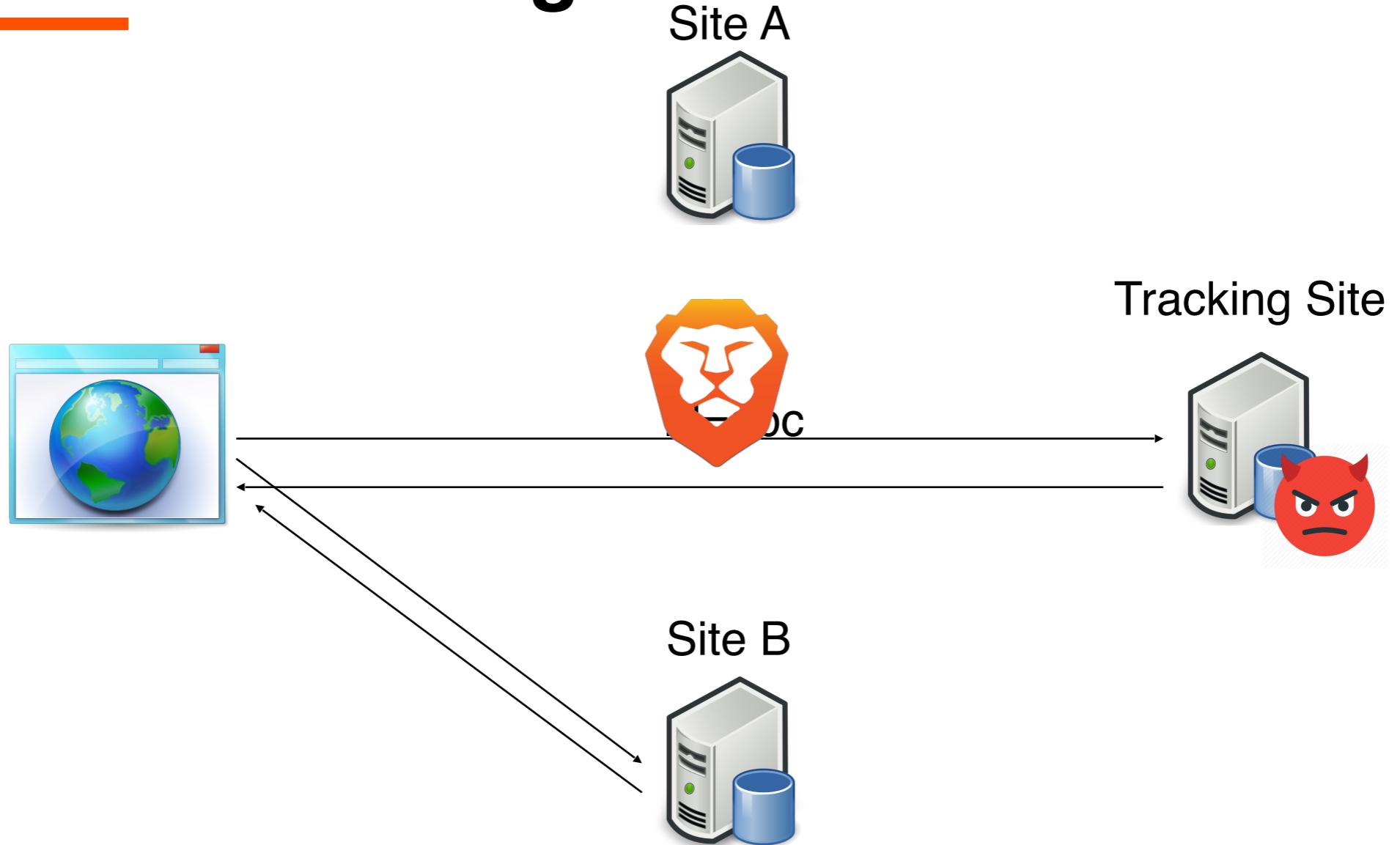
# Brave Blocks Tracking Cookies



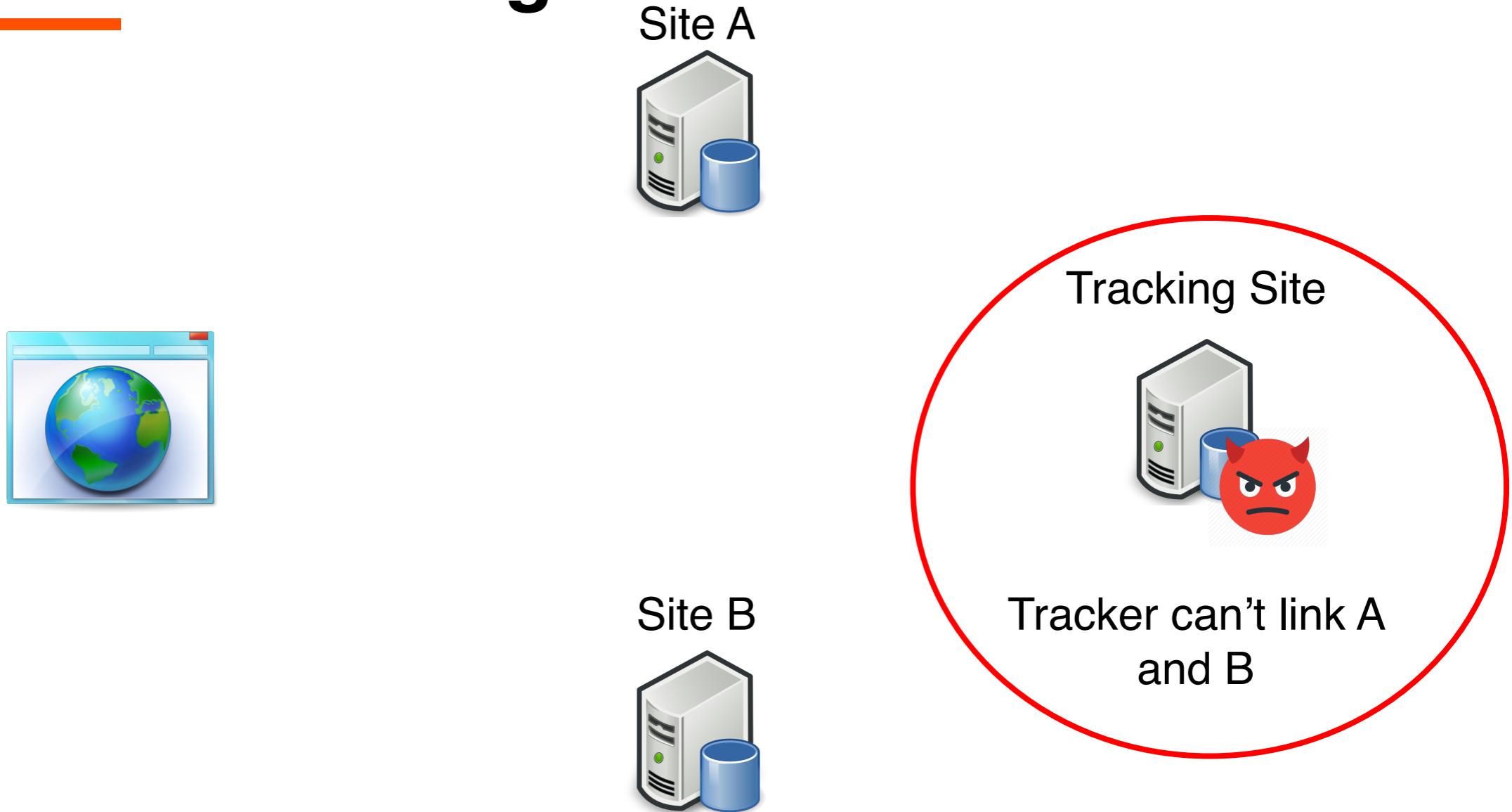
# Brave Blocks Tracking Cookies



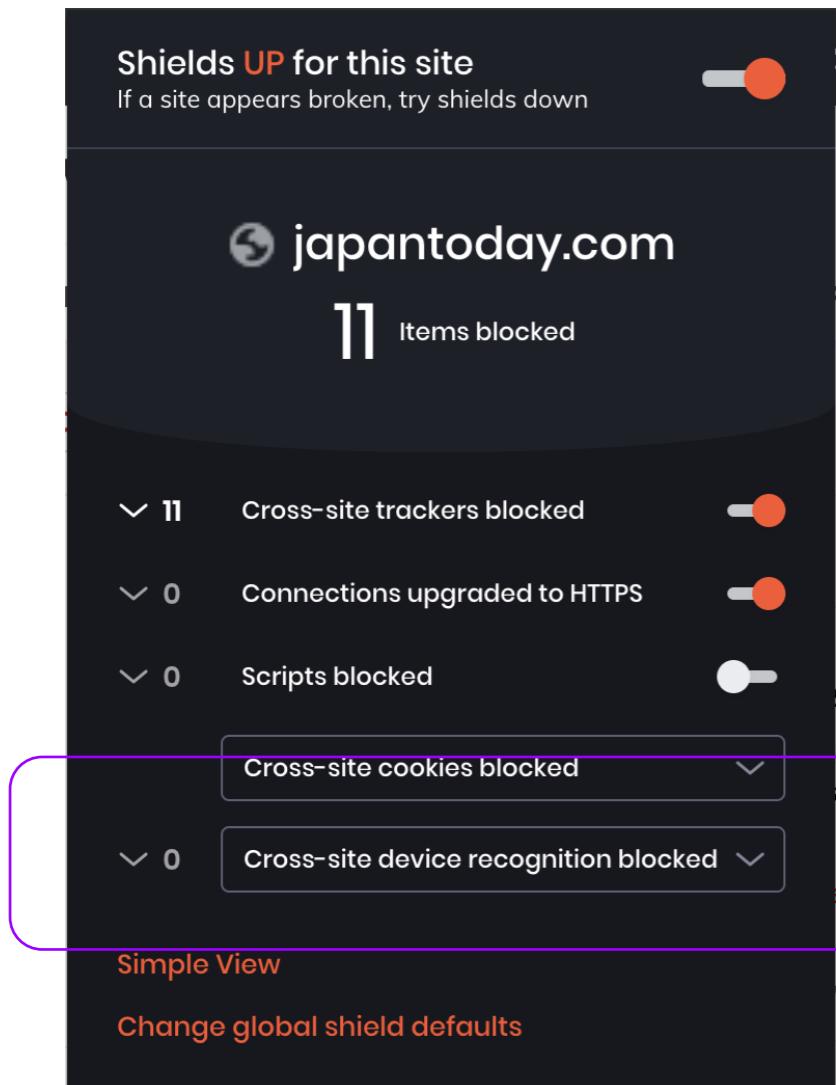
# Brave Blocks Tracking Cookies



# Brave Blocks Tracking Cookies



# Brave Privacy Protections



- Reduce finger printing vectors
- Currently:
  - Hardware identifiers
  - Canvas
  - WebGL
  - Audio
- Planned:
  - Fonts
  - User agent
  - Screen size

# **Under Exploration Possible Privacy Protections**

- Restrictions on third-party scripts
- Identifying tracking behaviors, not just scripts / URLs
- Query parameters filtering
- Bounce tracking
- Much more...

# Overview

1. Why websites track (and how much)
2. “Classic” tracking
3. Fingerprinting / “passive tracking”
4. Fingerprinting counter measures
5. Anti-finger printing exercise
6. Privacy protections in Brave
7. Wrapping up

# Unasked for Advice

- Brave is hiring, keep us in mind
- Privacy is more than just web, there's lots to do
- Don't accept privacy as a feature...
- Choose your employer with values in mind

# Thanks!

- **Pete Snyder**  
Privacy Researcher  
[pes@brave.com](mailto:pes@brave.com)  
@pes10k
- Questions?
  - Standards work?
  - Privacy jobs?
  - Brave business model
  - BAT / Block chain
  - Anything else?

