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?

2 CENTS PAY NO MORE!

Chicago Daily Tribune

THE WORLD'S GREATEST NEWSPAPER

FINAL

HUGE SWINDLE PLOT

Judge Orders Girl in 'Badger'

BALK INSURANCE COMPANY THEFT

Chicago Daily Tribune

THE WORLD'S GREATEST NEWSPAPER

FINAL

GOONS SMASH MEAT PLANT

Massed CIO Pickets Rout Police at So. St. Paul

YOUNGDAHL SIDESTEPS AID PLEAS

Defy Writ, Bar Workers

U.S. Heiress Killed in Plane Crash

PLAYING WITH THE SCISSORS AGAIN

TRUMAN ASKS 2½ BILLIONS MORE; EUROPEAN AID PLAN IS ASSAILED

Spending Called 'Utter Folly,' 'Waste'

HOUSE PASSES BILL TO COMPEL U.S. AIDS TO TALK

Air Force, Army, Navy to Get Shares

TAYLOR . . . big ambition

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

Regular skipper Eoin Morgan misses the game to play in the IPL.

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

Notts star Taylor said: "We must put the World Cup behind us — and ignore it but learn from it. This is a fresh start."

England's 13-man squad has five uncapped players: Kent keeper/batsman Sam Billings, Surrey all-rounder Zafar Ansari, Somerset seamer Lewis Gregory, Northants all-rounder David Willey and Hampshire batsman James Vince.

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

[illegible]

Kid Dan's ton of fun

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

The 17-year-old hit 161 in only his second first-class fixture as Essex racked up 450-8 against Surrey at The Oval.

Kent's Godfrey Bryan in 1920 and Dipak Patel for Worcestershire in 1976 are believed to have hit tons when younger than Lawrence, whose previous highest score was ten.

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

Lee: Oui will return

By JONNY FORDHAM

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

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

Dickson's Premiership leaders Northampton were KO'd by Clermont, but the England 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

SMOKIN' JOE . . . Root is red-hot

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 FEC – Future England Captain.

[illegible]

MAY THE SAUCE BE WITH YOU

ALL ROOTS lead to the cricket! England batsman Joe Root met up with super sauce maker Levi Roots ahead of the Third Test against West Indies in Barbados on Friday. Let's hope it's a spicy affair.

[illegible]

That's the sort of cheeky fun we like from Joe Root.

BRIGHTON'S summer transfer policy may have to take a hit after chairman Tony Bloom's bet of misfortune.

The Seagulls supremo placed £13,000 on himself to finish the Brighton Marathon in no more than 3hr 45 mins — only to cross the line four minutes and 30 seconds later.

VIEW TO A DILL

ANDREW DILLON

Cough not that Good

EVERTON is known as the school of science but they have been turning their hands to amateur dramatics too.

[illegible]

Ooh, suits you Shaun

SHAUN MURPHY'S garish suits have been dazzling fans, TV crews and players at snooker's world championship.

But spokesman for tournament sponsors Betfred, Mark 'Stuart' Pearson, told VTAD: "Every time we sponsor a horserace we give a prize for the best-dressed nag, taking into account coat, condition and colours. It's similar with Shaun."

Murphy will then be given a cheque for the Royal Manchester Children's Hospital.

A 'Parker' can cut it

SOMETHING for the weekend, sir?

[illegible]

[illegible]

WORLD SNOOKER

BAD TABLE MANNERS . . . Ronnie puts chalk down

CHALK OF SHAME

O'Sullivan in dust-up

By HARRY TALBOT

RONNIE O'SULLIVAN is caught in a World Snooker probe after breaking the rules in his quarter-final clash with Stuart Bingham.

The five-time world champ placed his chalk on the table to line up a shot but was **NOT** reprimanded by referee Terry Camilleri.

[illegible]

JUDD HEA-DING THROUGH

TRUMP . . . on a roll

JUDD TRUMP put China's No.1 Ding Junhui to the sword as he moved to within a frame of the Crucible semi-finals.

The Juddernaut leads world No.3 Ding 12-4 to take another massive stride towards his first world title.

After his best season that has seen titles in Australia and at the World Grand Prix in Llandudno, 25-year-old Trump rattled in breaks of 54, 82, 94, 106, 76, [illegible] 55, 127 and 111 to leave Ding in a daze.

NEIL ROBERTSON faces a fight to make the last four as he lost four frames on the spin to trail Barry Hawkins [illegible]

In the final quarter-final SHAUN MURPHY leads Anthony McGill 9-7 after winning the final three frames of last night's session.

Pep gets Klopped

From ANTONY KASTRINAKIS

JURGEN KLOPP wrecked Pep Guardiola's Treble bid as ten-man Borussia Dortmund beat Bayern Munich on penalties in the German Cup semi-finals.

Dortmund won the shootout 2-0 at the Allianz Arena, with the game ending 1-1 after extra-time.

Robert Lewandowski's opener against his old club was cancelled out by Pierre-Emerick Aubameyang's 75th-minute leveller for Dortmund.

Outgoing Dortmund boss Klopp, wanted by a host of Premier League clubs, saw Kevin Kampl sent off for a second booking late on.

£30m CUP DEAL

From Back Page

144-year history that full naming rights have been granted.

US drinks giant Budweiser – who paid £8m a year merely to be "in association with" the trophy FA Cup – ended their three-year partnership last year.

But the Emirates deal is a complete rebranding that will upset the purists.

Lawrie McMenemy, who guided Second Division Southampton [illegible] in 1976, quipped: "It's the one and only, it's **THE** FA Cup and it would be a pity to see it lose that tradition, not just in our game but in the game worldwide. It was the biggest and the best. But football today is solely about money, money, money."

McMenemy (above) added: "I would have thought there was enough money circulating in football in TV rights to avoid this. Football is about history and tradition. Our Cup was different. No other country had anything to compare with it."

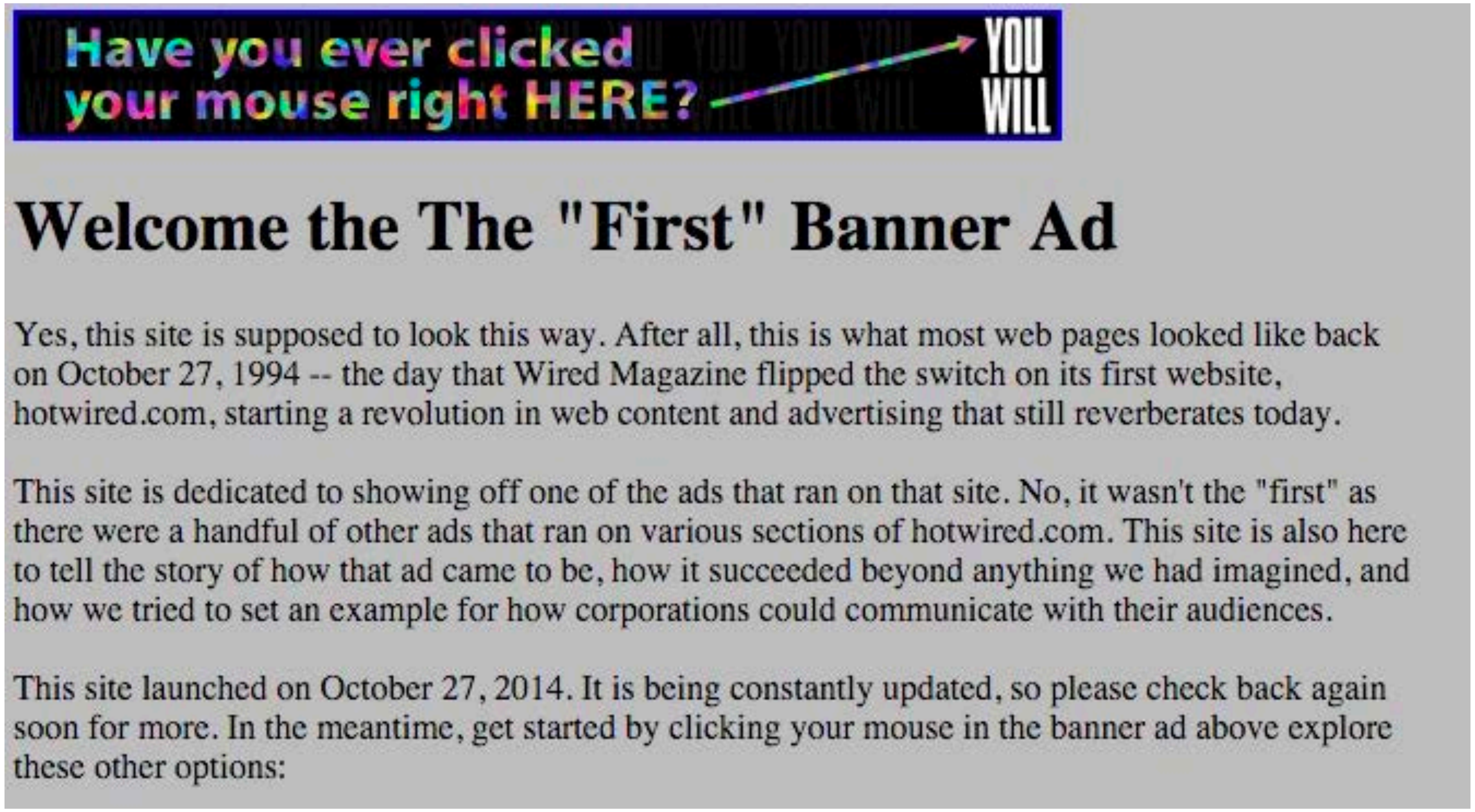
Football fans also took to Twitter last night, calling the deal "awful", "horrible" and "bull-dozing our football".

With this year's competition not having a sponsor, FA commercial director Stuart Turner and his team have had to offer full naming rights to secure a new £10m-a-year [illegible]

[illegible] Emirates – sponsors of current Cup holders Arsenal's [illegible] – made their move [illegible] £10m-a-year relationship [illegible]

An FA spokesman admitted [illegible] continue to have discussions with a number of parties about FA Cup partner opportunities."

100%
FREE
MAGAZINE
SUBSCRIPTIONS!
GQ
SOUND + STYLE
A CELEBRATION OF MUSIC AND FASHION
CHANCE THE RAPPER
THE WEEKND
OBAMA VS. TRUMP
THE NEW COLD WAR
HELL ON WHEELS
Golf
BUST IT EVERY TIME
AMERICA'S 100 GREATEST COURSES+
GLAMOUR
WOMEN
People
How Brad's Movie



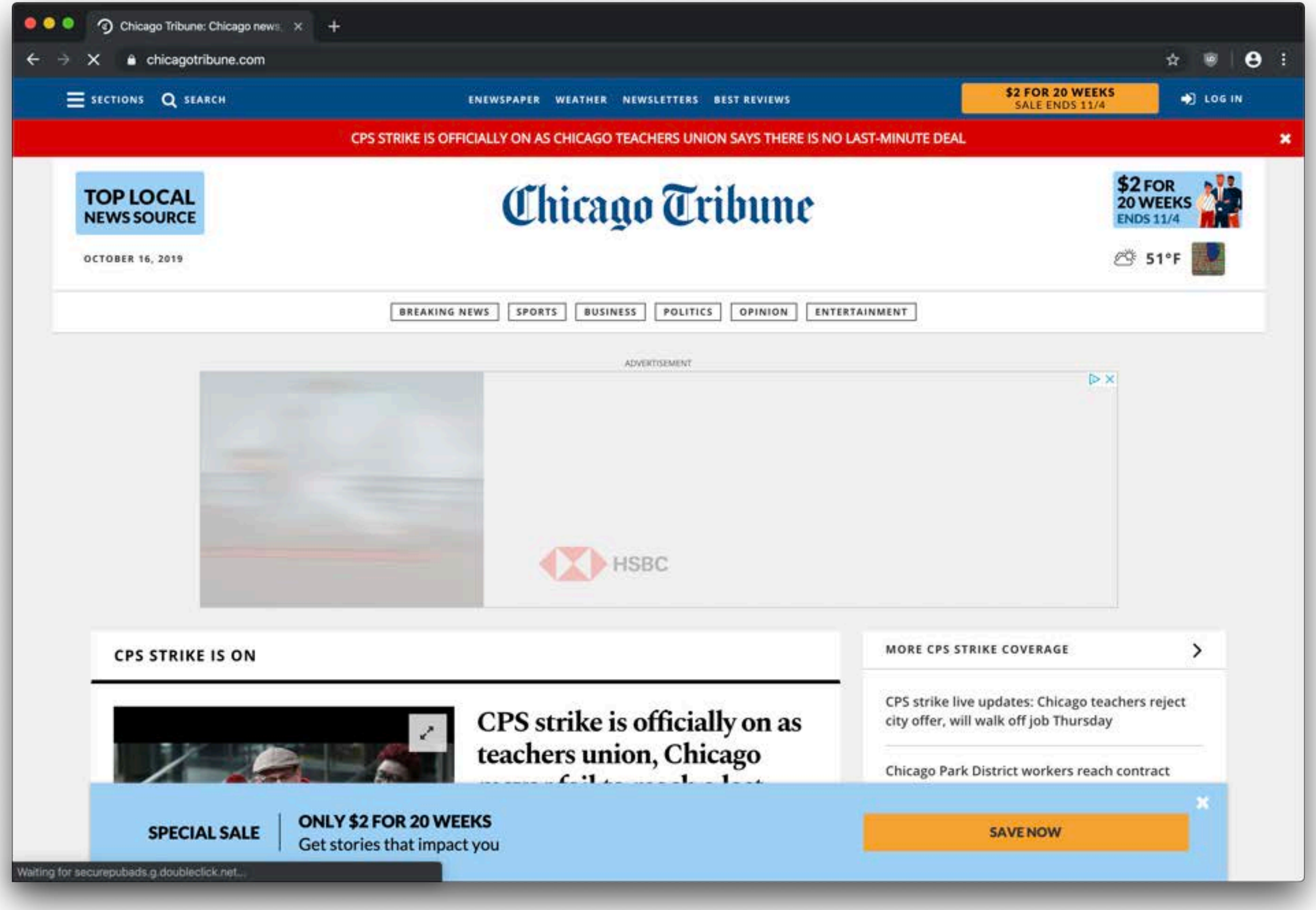
Welcome the The "First" Banner Ad

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:

Disney Lover's
Web Ring
Previous | Next | Random | List Sites



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

OCTOBER 16, 2019

CPS STRIKE IS ON

CPS strike is officially on as teachers union, Chicago mayor fail to reach a last

MORE CPS STRIKE COVERAGE

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

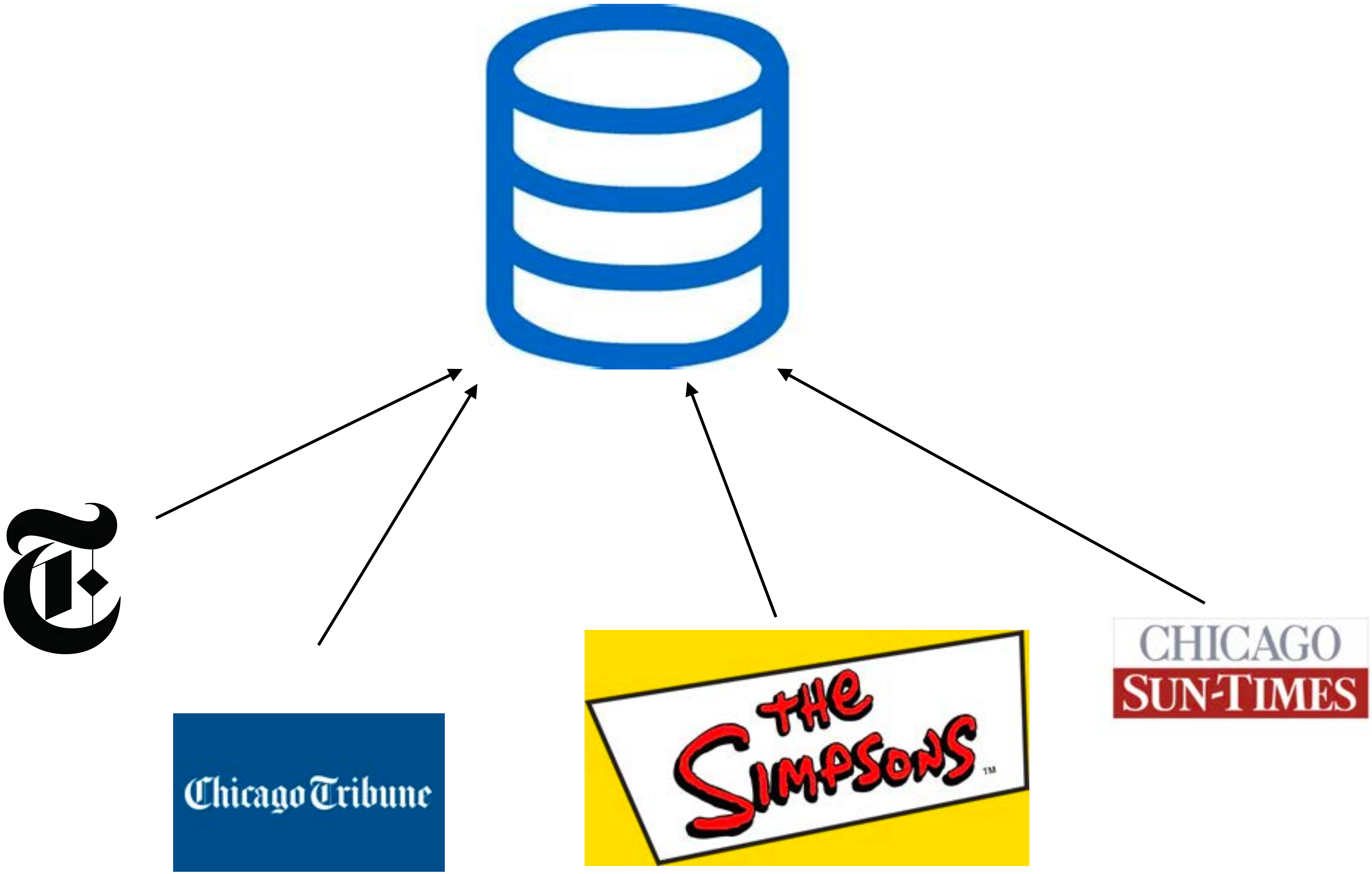
Chicago Park District workers reach contract

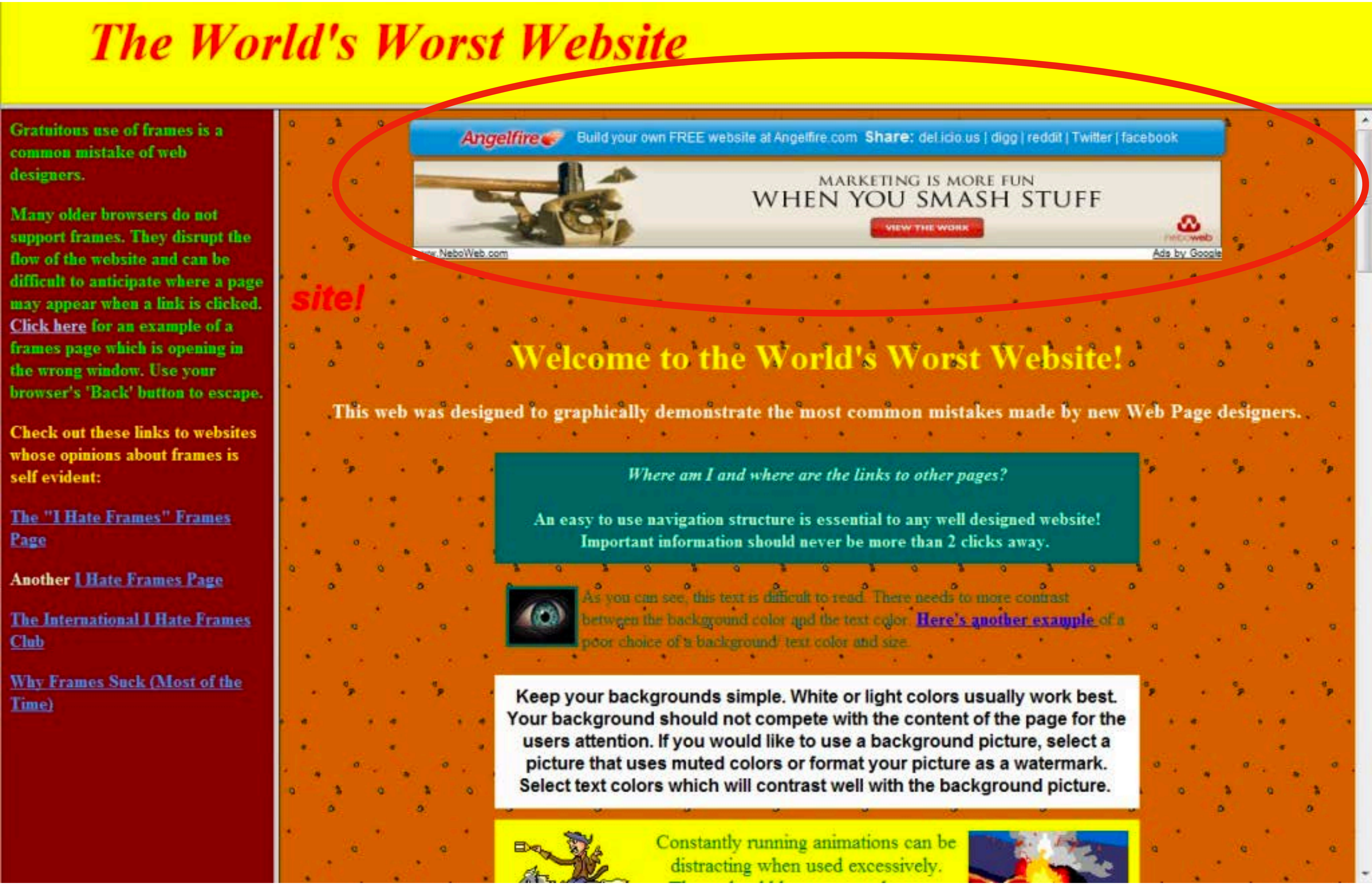
SPECIAL SALE

ONLY $2 FOR 20 WEEKS

Get stories that impact you

SAVE NOW


Chicago Tribune
The Simpsons™
CHICAGO SUN-TIMES



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)

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.

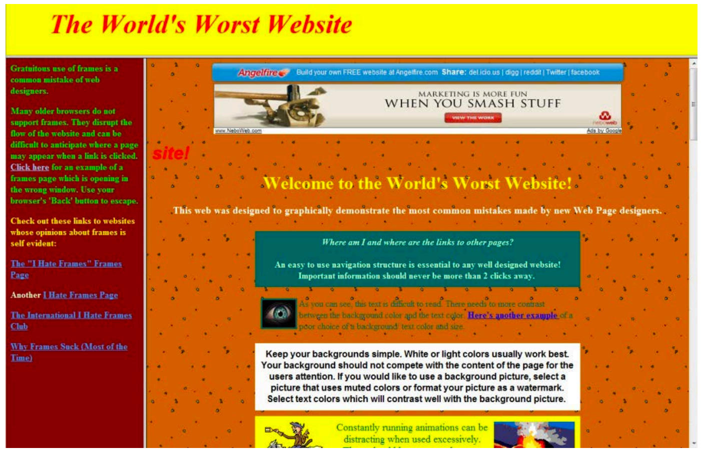
As you can see, this text is difficult to read. There needs to more contrast between the background color and the text color. Here's another example of a poor choice of a background/ text color and size.

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 Tribune

CHICAGO
SUN-TIMES



The World's Worst Website

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
www.NeboWeb.com
Ads by Google
site!

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)

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.

$ $ $

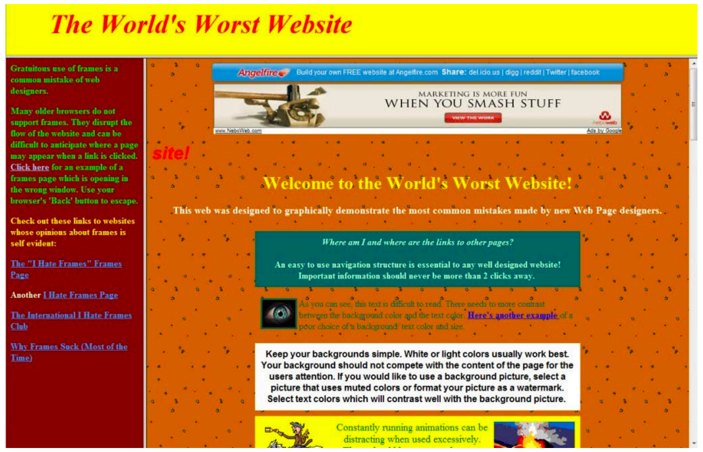
¢ ¢ ¢

Chicago Tribune

CHICAGO
SUN-TIMES

$

→



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)

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.

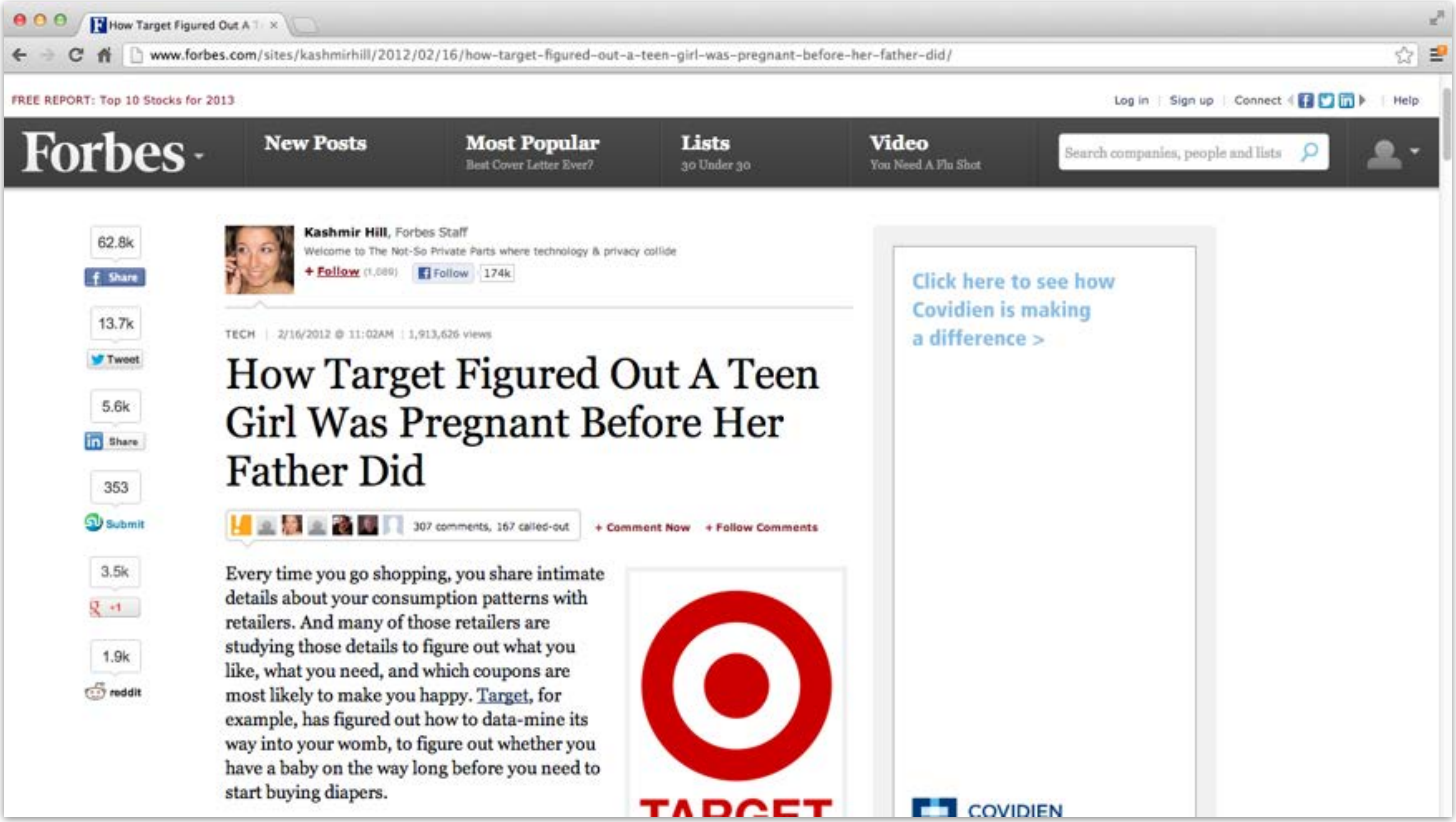
Chicago Tribune

CHICAGO SUN-TIMES

BREITBART

Identify “expensive” people here

Pay a little to advertise to them here


How Target Figured Out A T
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
Best Cover Letter Ever?
Lists
30 Under 30
Video
You Need A Flu Shot
Search companies, people and lists
62.8k
Share
13.7k
Tweet
5.6k
Share
353
Submit
3.5k
+1
1.9k
reddit
+ Follow (1,089)
Follow
174k
307 comments, 167 called-out
+ Comment Now
+ Follow Comments
Click here to see how Covidien is making a difference >
COVIDIEN
TARGET

Kashmir Hill, Forbes Staff

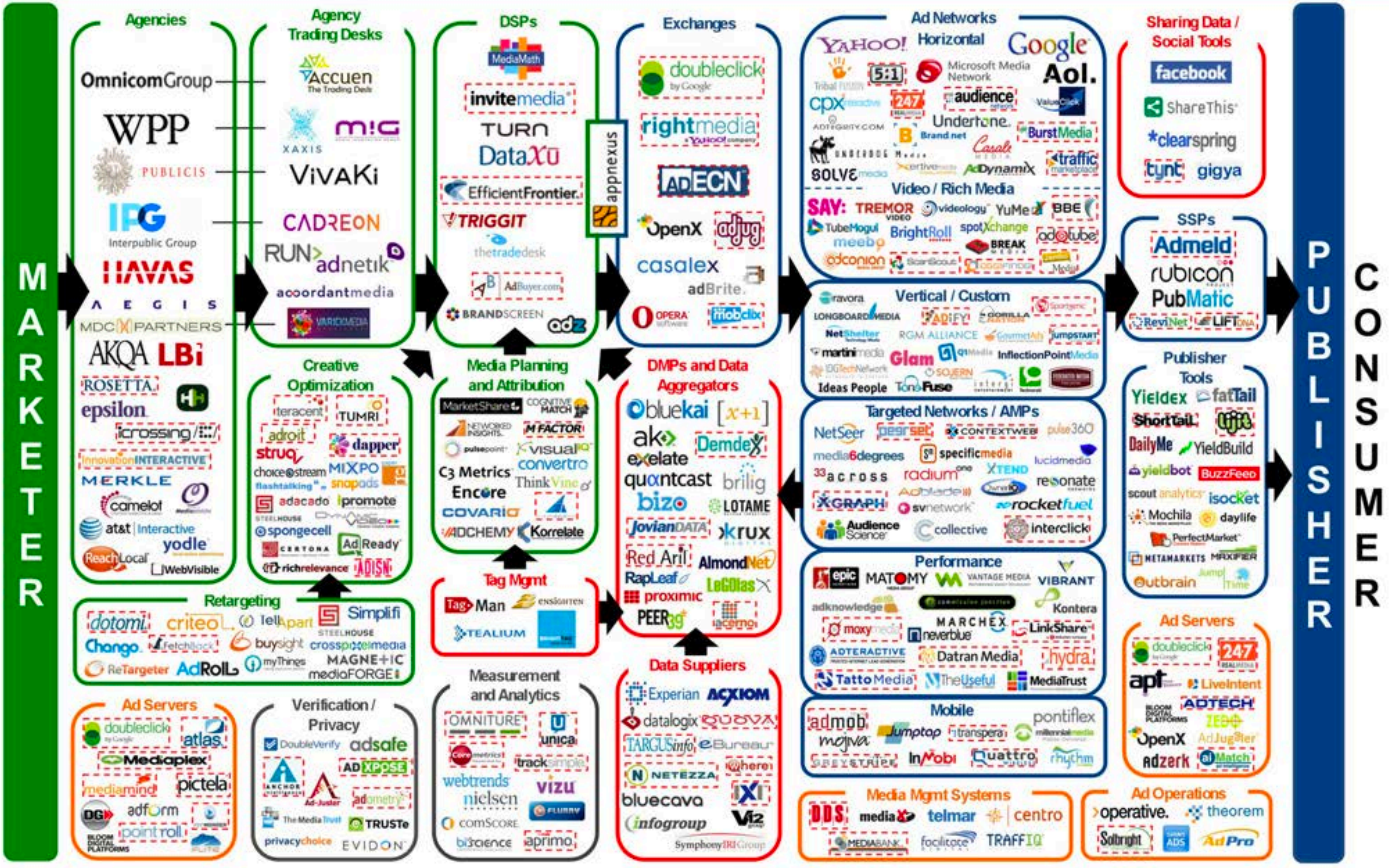
Welcome to The Not-So Private Parts where technology & privacy collide

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

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

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.

DISPLAY LUMAscape



MARKETER

Agencies: OmnicomGroup, WPP, Publicis, IPG Interpublic Group, HAVAS, AEGIS, MDC Partners, AKQA, LBi, Rosetta, epsilon, iCrossing, Innovation Interactive, Merkle, camelot, at&t Interactive, yodle, ReachLocal, WebVisible

Agency Trading Desks: Accuen The Trading Desk, XAXIS, M!G, VivaKi, CADREON, RUN, adnetik, accordantmedia, Varick Media

DSPs: MediaMath, invitemedia, TURN, DataXu, EfficientFrontier, TRIGGIT, thetradedesk, AdBuyer.com, BRANDSCREEN, adz, appnexus

Exchanges: doubleclick by Google, rightmedia a Yahoo! company, ADECN, OpenX, adjug, casalex, adBrite, OPERA software, mobclix

Ad Networks

Horizontal: YAHOO!, Google, Tribal Fusion, 5:1, Microsoft Media Network, Aol., cpx interactive, 24/7 Real Media, audience science, ValueClick, Adiquity.com, Undertone, Brand.net, Casale Media, BurstMedia, Underdog Media, Vertive Media, AdDynamix, traffic marketplace, SOLVE media

Video / Rich Media: SAY, TREMOR VIDEO, videology, YuMe, BBE, TubeMogul, BrightRoll, spotXchange, adotube, meebo, BREAK MEDIA, adconion, ScanScout

Vertical / Custom: gravora, Sportgenic, LONGBOARD MEDIA, FADIFY, GORILLA NATION, NetShelter, RGM ALLIANCE, jumpstart, martini media, Glam, InflectionPoint Media, IDG TechNetwork, SOJERN, Ideas People, Tonto, Fuse, Interclick

Targeted Networks / AMPs: NetSeer, peerset, CONTEXTWEB, pulse360, media6degrees, specificmedia, lucidmedia, 33across, radiumone, XTEND, resonate, Adblade, XGRAPH, svnetwork, rocketfuel, Audience Science, collective, interclick

Performance: epic, MATOMY, VANTAGE MEDIA, VIBRANT, adknowledge, Kontera, moxy media, MARCHEX, neverblue, LinkShare, ADTERACTIVE, Datran Media, hydra, TattoMedia, TheUseful, MediaTrust

Mobile: admob, pontiflex, mojiva, Jumptap, transpera, millennial media, GREYSTRIPE, InMobi, Quattro, rhythm

Sharing Data / Social Tools: facebook, ShareThis, clearspring, tynt, gigya

SSPs: Admeld, rubicon project, PubMatic, ReviNet, LIFT DNA

Publisher Tools: Yieldex, fatTail, ShortTail, DailyMe, YieldBuild, yieldbot, BuzzFeed, scout analytics, isocket, Mochila, daylife, PerfectMarket, METAMARKETS, MAXIFIER, Outbrain, Jump Time

Ad Servers: doubleclick by Google, 24/7 Real Media, apt, LiveIntent, Bloom Digital Platforms, ADTECH, ZEDO, OpenX, AdJuggler, adzerk, Match

Creative Optimization: teracent, TUMRI, adroit, struq, dapper, choicestream, MIXPO, flashtalking, snapads, adacado, ipromote, STEELHOUSE, DynamicLogic, spongecell, CERTONA, AdReady, richrelevance, ADISN

Media Planning and Attribution: MarketShare, COGNITIVE MATCH, NETWORKED INSIGHTS, M FACTOR, pulsepoint, visualIQ, convertro, C3 Metrics, Encore, ThinkVine, COVARIO, ADCHEMY, Korrelate

Tag Mgmt: TagMan, ensighten, TEALIUM

DMPs and Data Aggregators: bluekai, [x+1], akamai, Demdex, exelate, quantcast, brilig, bizo, LOTAME, JovianDATA, krux, Red Aril, AlmondNet, RapLeaf, LoGDias, proximic, PEER39, Lucemo

Data Suppliers: Experian, ACXIOM, datalogix, QUOVA, TARGUSinfo, eBureau, here, NETEZZA, bluecava, IXI, infogroup, V12 group, SymphonyIRIGroup

Retargeting: dotomi, criteo, TellApart, Simplifi, STEELHOUSE, Chango, FetchBack, buysight, crosspixelmedia, ReTargeter, AdRoll, myThings, MAGNETIC, mediaFORGE

Ad Servers: doubleclick by Google, atlas, Mediaplex, mediamind, pictela, DG, adform, pointroll, Bloom Digital Platforms, Flite

Verification / Privacy: DoubleVerify, adsafe, ANCHOR, AD XPOSE, Ad-Juster, adometry, The Media Trust, TRUSTe, privacychoice, EVIDON

Measurement and Analytics: OMNITURE, unica, Core metrics, tracksimple, webtrends, vizu, nielsen, FLURRY, comScore, bizsence, aprimo

Media Mgmt Systems: DDS, mediaocean, telmar, centro, MEDIABANK, facilitate digital, TRAFFIQ

Ad Operations: operative., theorem, Solbright, Smart ADS, AdPro

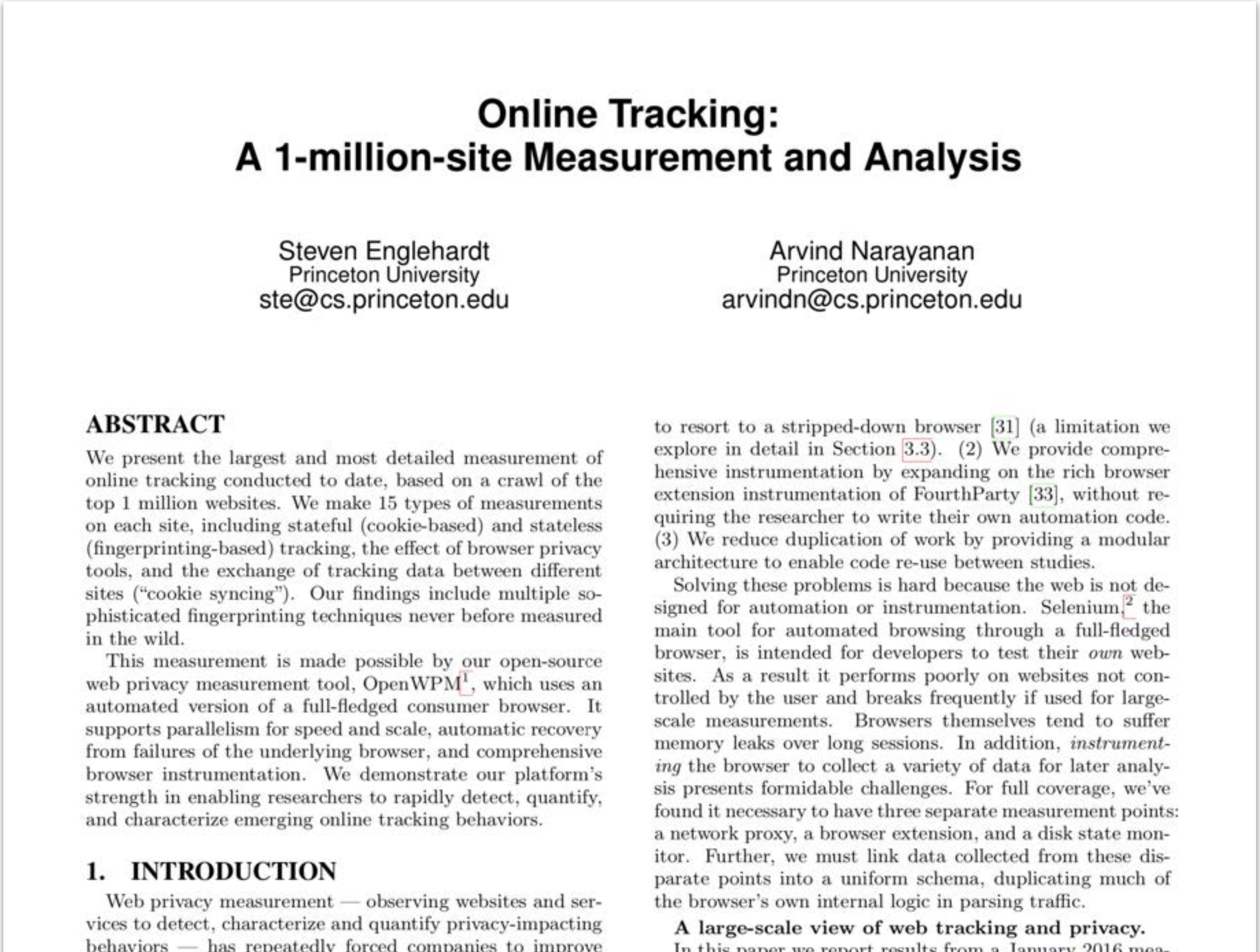
PUBLISHER

CONSUMER

LUMA partners

Denotes acquired company

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[1], 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.

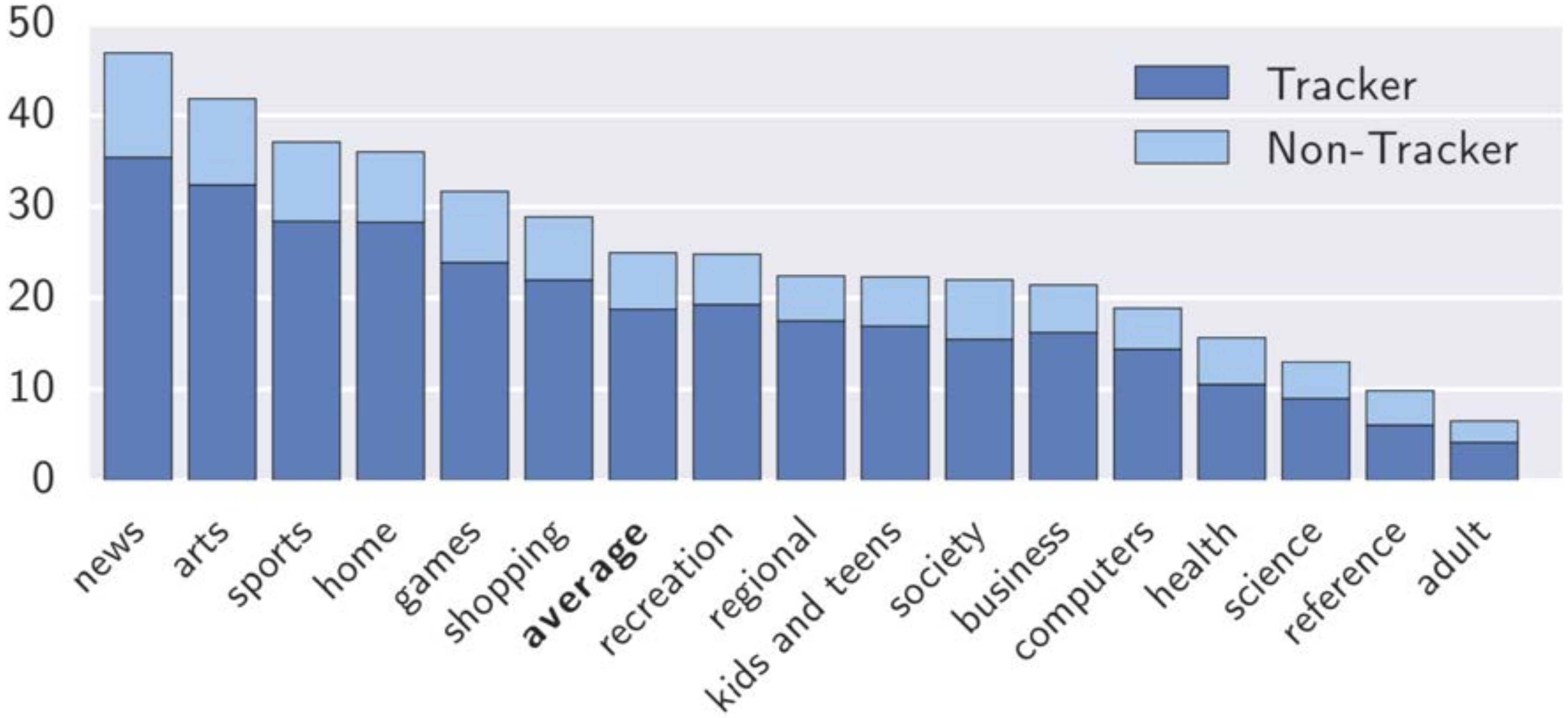
1. INTRODUCTION

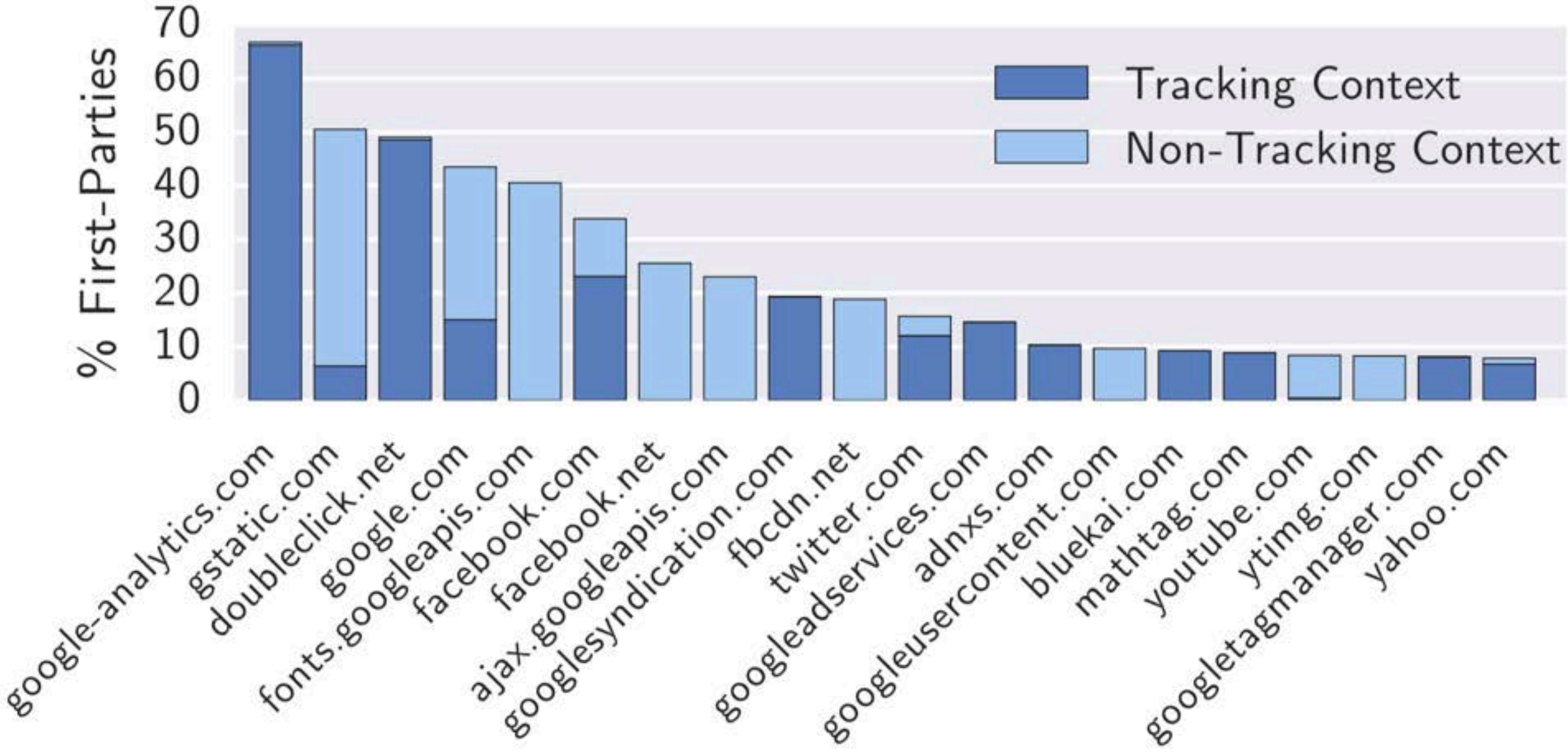
Web privacy measurement — observing websites and services to detect, characterize and quantify privacy-impacting behaviors — has repeatedly forced companies to improve

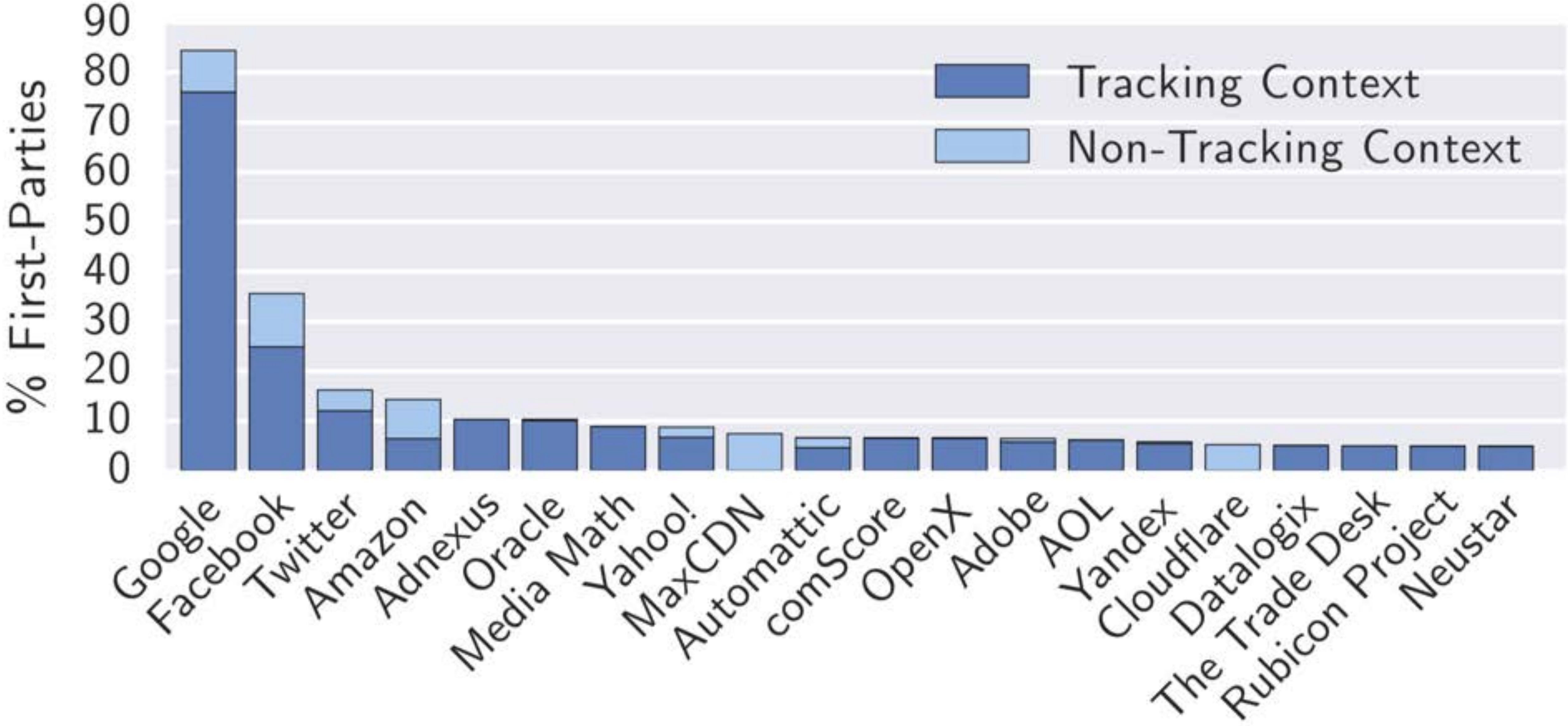
to resort to a stripped-down browser [31] (a limitation we explore in detail in Section 3.3). (2) We provide comprehensive instrumentation by expanding on the rich browser extension instrumentation of FourthParty [33], without requiring the researcher to write their own automation code. (3) We reduce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


50
40
30
20
10
0
Tracker
Non-Tracker
news
arts
sports
home
games
shopping
average
recreation
regional
kids and teens
society
business
computers
health
science
reference
adult


% First-Parties
0
10
20
30
40
50
60
70
Tracking Context
Non-Tracking Context
google-analytics.com
gstatic.com
doubleclick.net
google.com
fonts.googleapis.com
facebook.com
facebook.net
ajax.googleapis.com
googlesyndication.com
fbcdn.net
twitter.com
googleadservices.com
adnxs.com
googleusercontent.com
bluekai.com
mathtag.com
youtube.com
ytimg.com
googletagmanager.com
yahoo.com

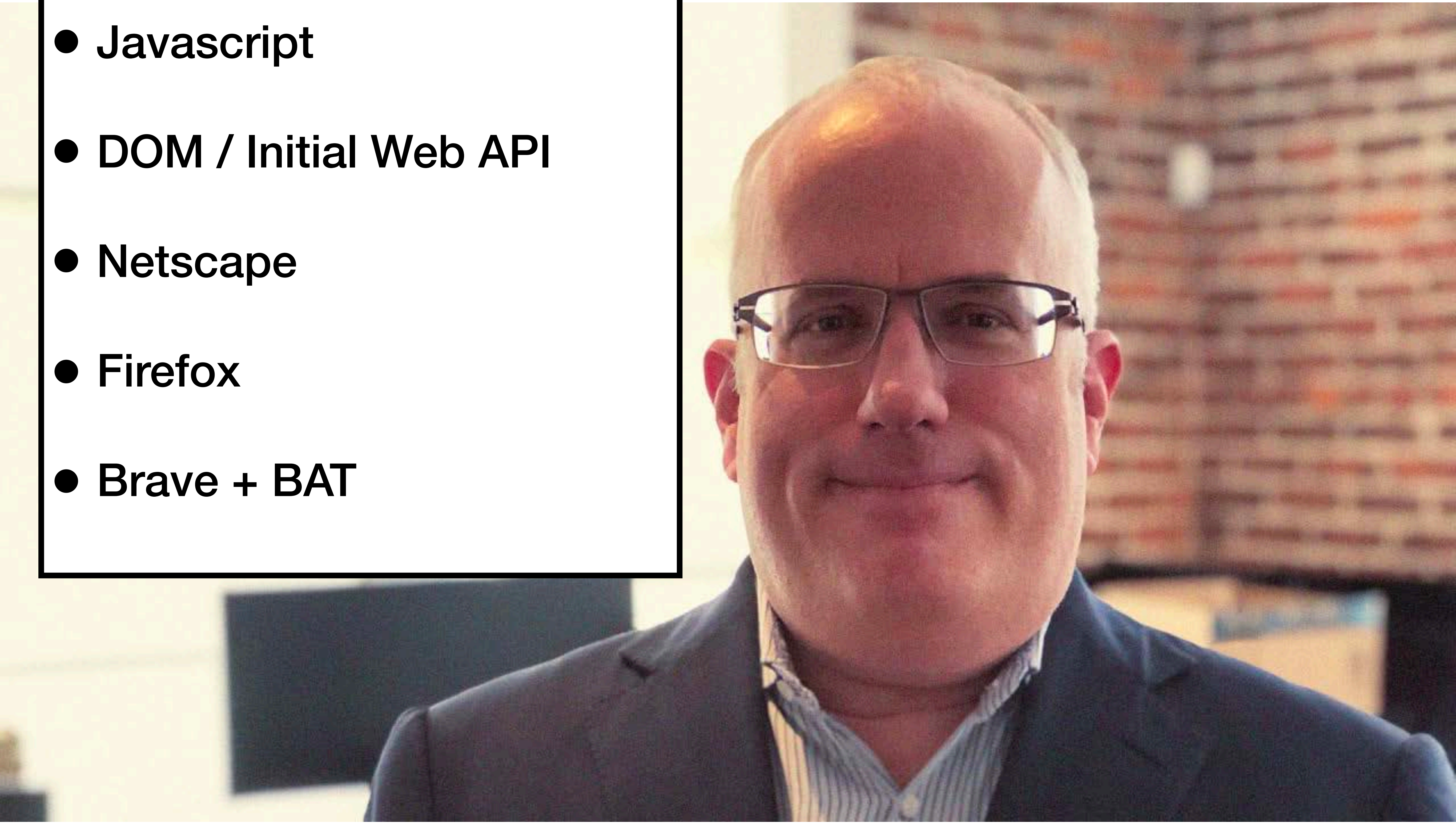

% First-Parties
90
80
70
60
50
40
30
20
10
0
Tracking Context
Non-Tracking Context
Google
Facebook
Twitter
Amazon
Adnexus
Oracle
Media Math
Yahoo!
MaxCDN
Automattic
comScore
OpenX
Adobe
AOL
Yandex
Cloudflare
Datalogix
The Trade Desk
Rubicon Project
Neustar

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

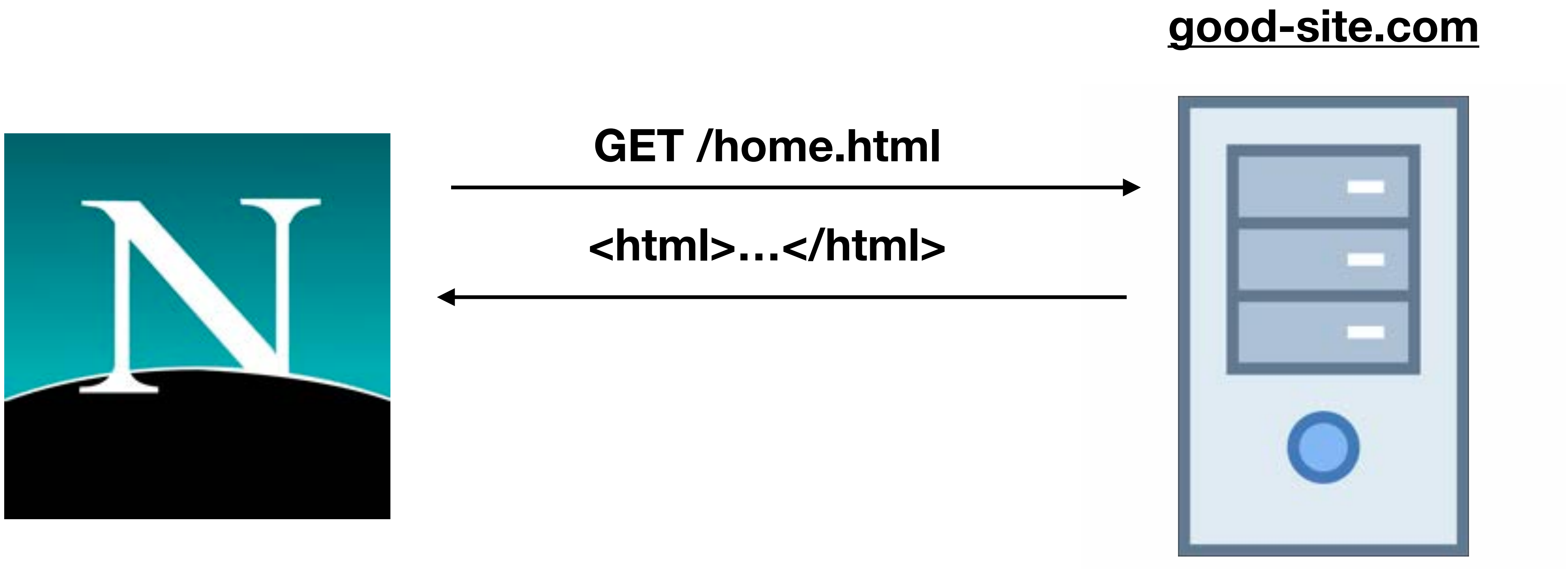


- Javascript
- DOM / Initial Web API
- Netscape
- Firefox
- Brave + BAT

Web 0.0

good-site.com

Web 0.0

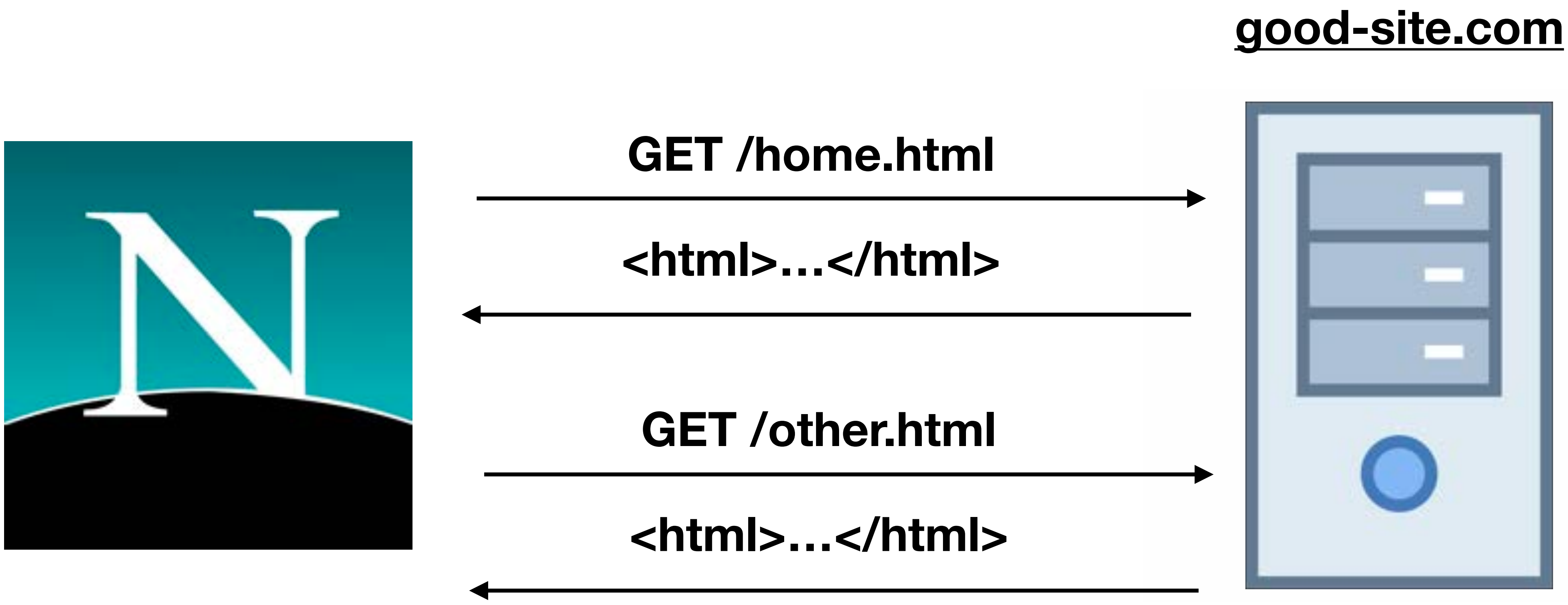


good-site.com

GET /home.html

<html>...</html>

Web 0.0



good-site.com

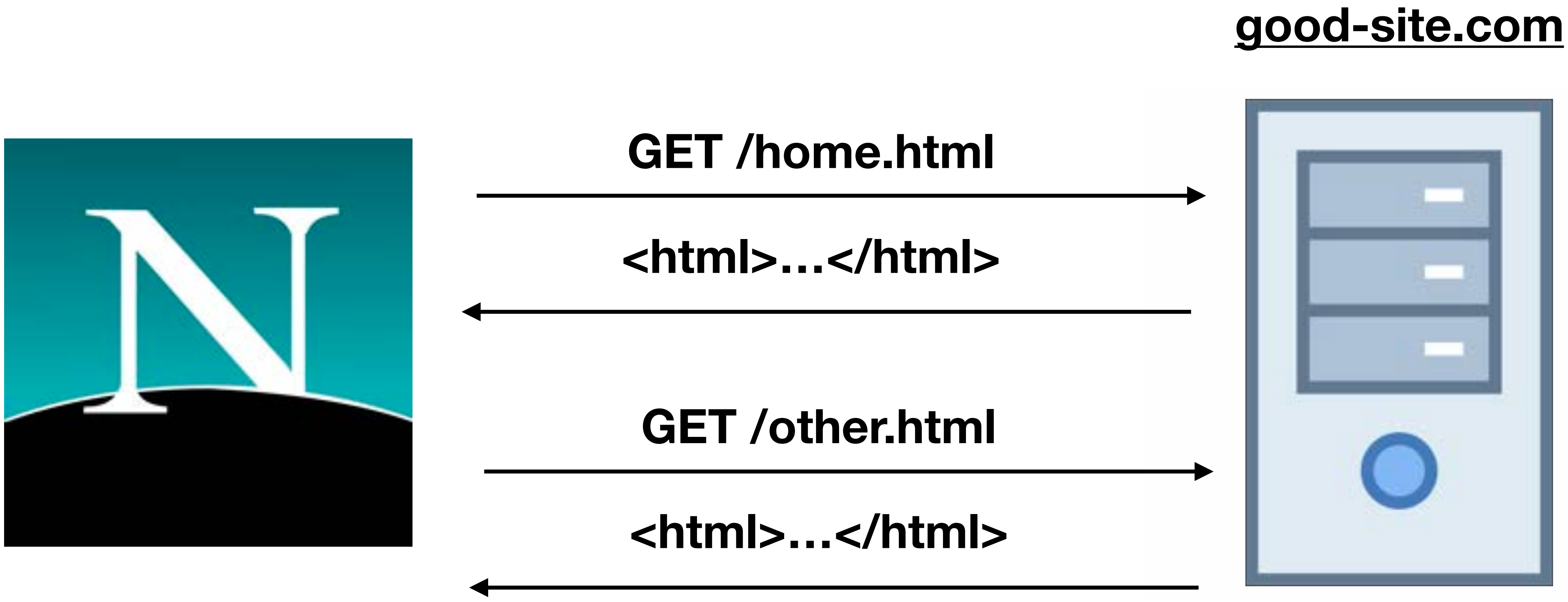
GET /home.html

<html>…</html>

GET /other.html

<html>…</html>

Web 0.0



good-site.com

GET /home.html

<html>…</html>

GET /other.html

<html>…</html>

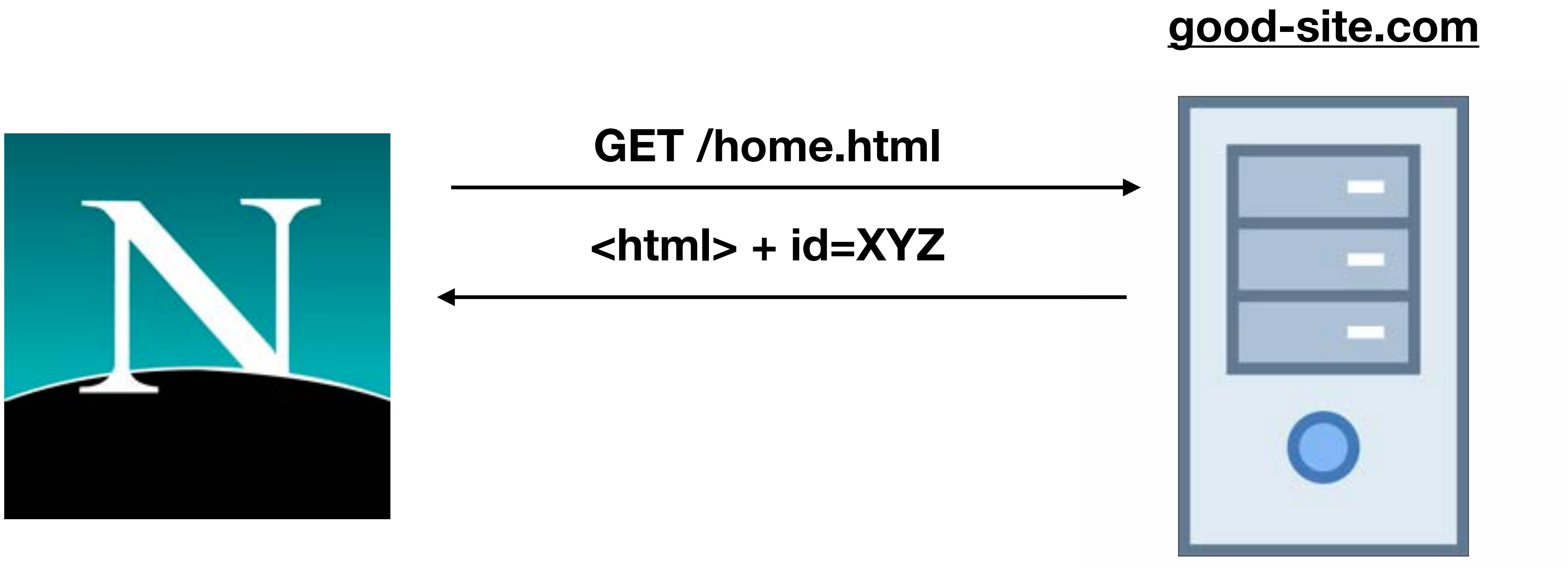
Birth of the Tracking

- **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

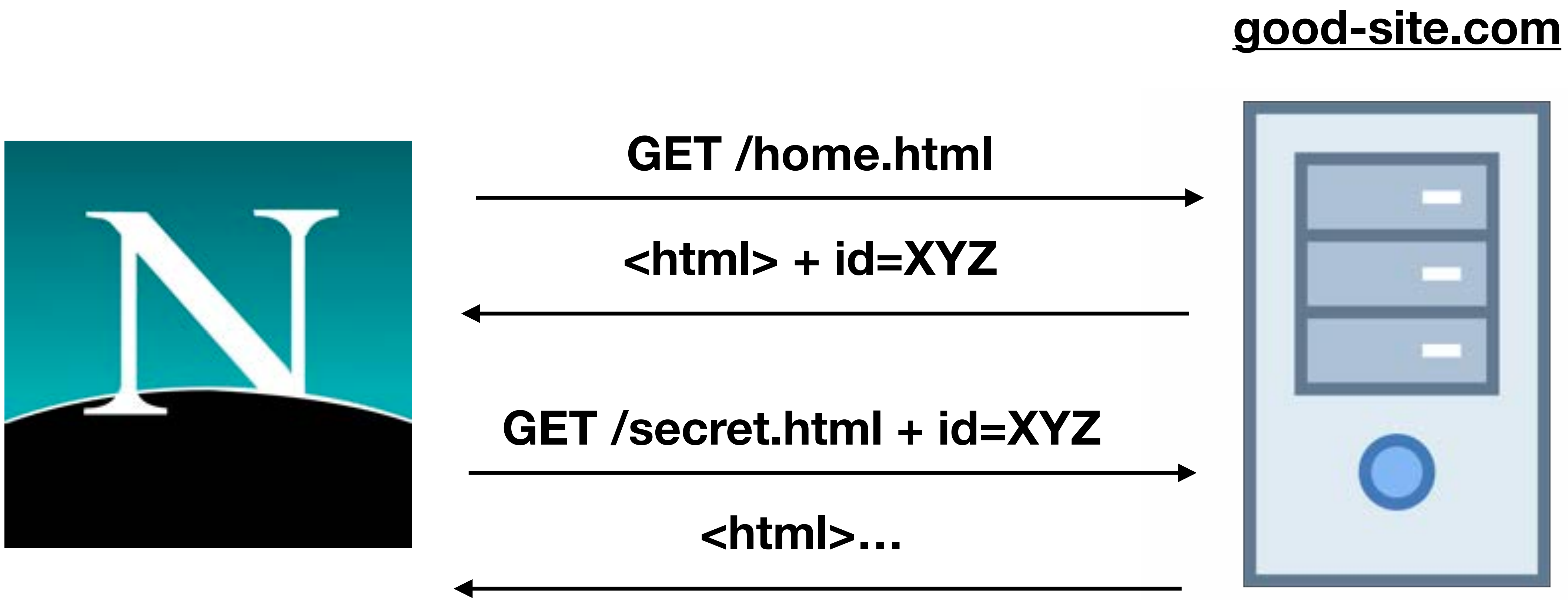


good-site.com

GET /home.html

<html> + id=XYZ

Web 0.0



good-site.com

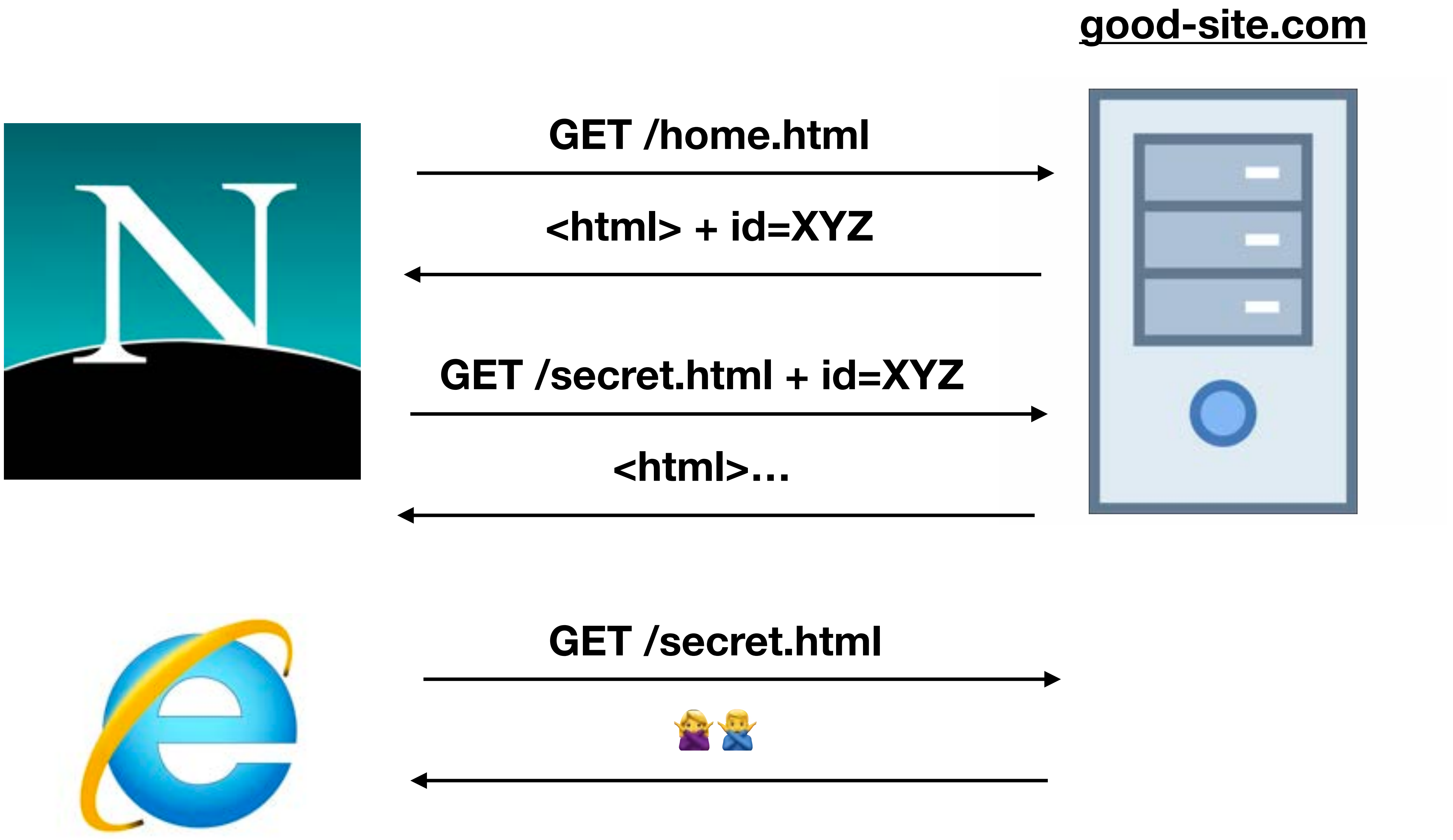
GET /home.html

<html> + id=XYZ

GET /secret.html + id=XYZ

<html>…

Web 0.0



good-site.com

GET /home.html

<html> + id=XYZ

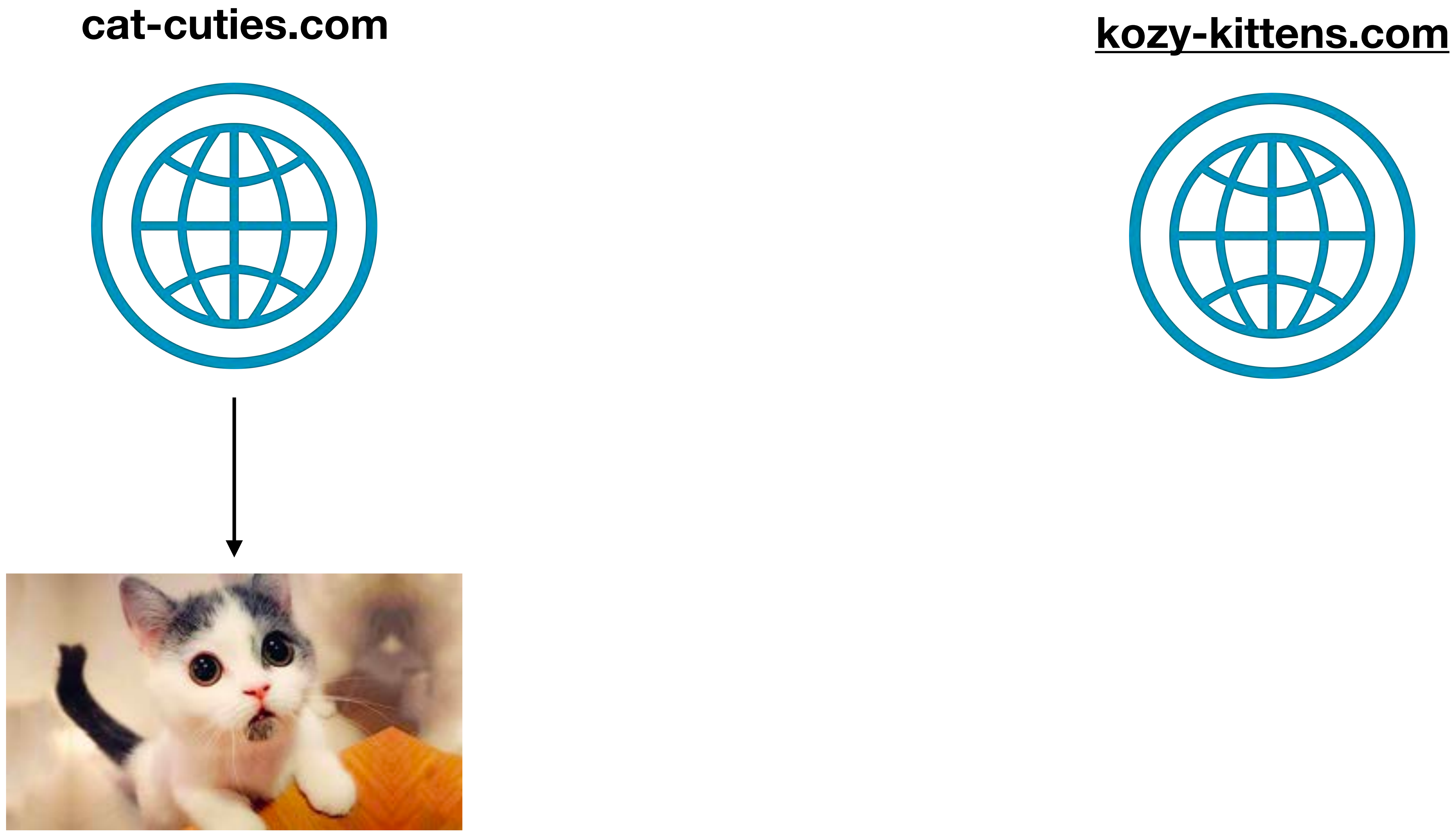
GET /secret.html + id=XYZ

<html>...

GET /secret.html

🙅‍♀️🙅‍♂️

But in the meantime…

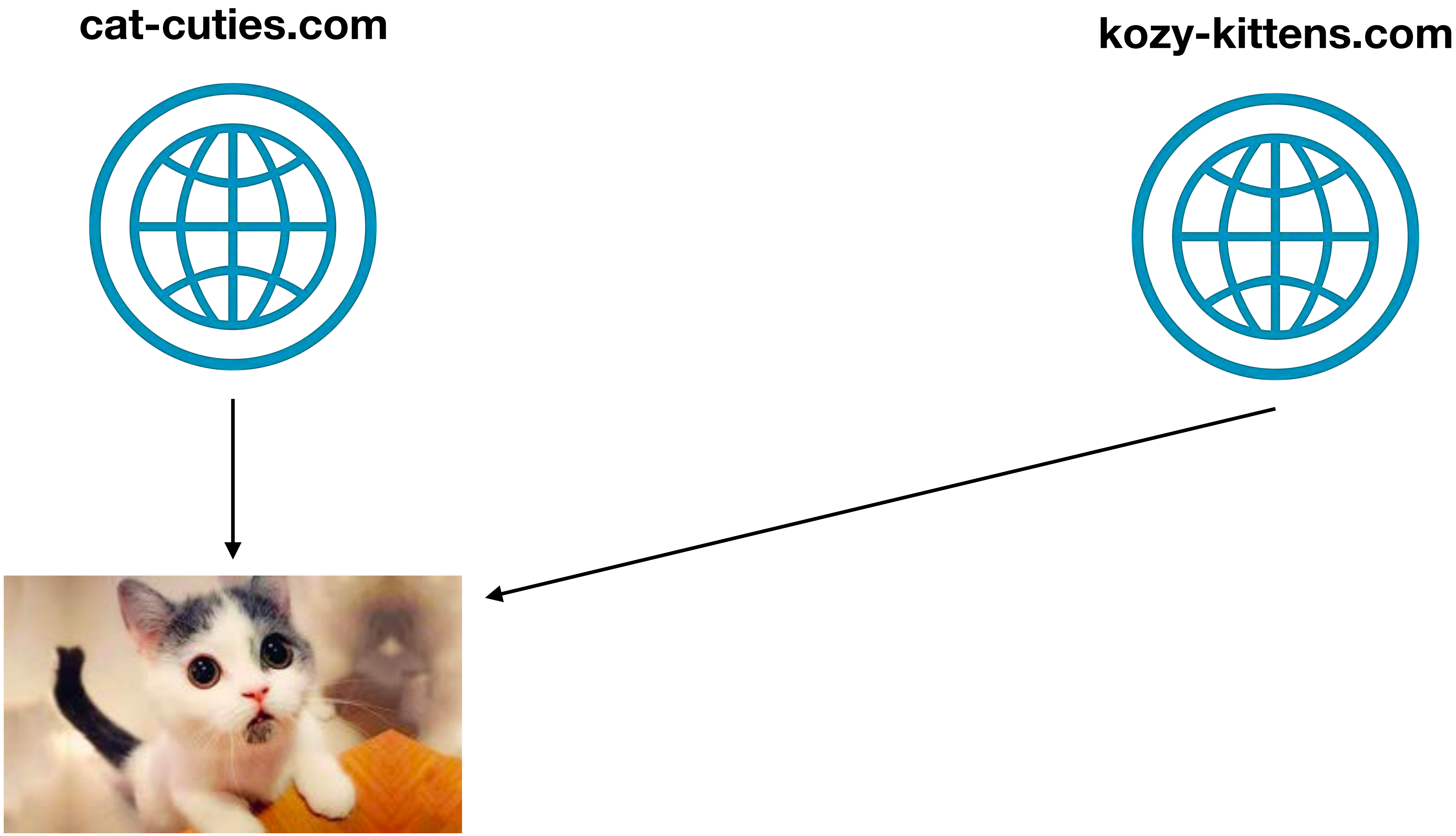


cat-cuties.com

kozy-kittens.com

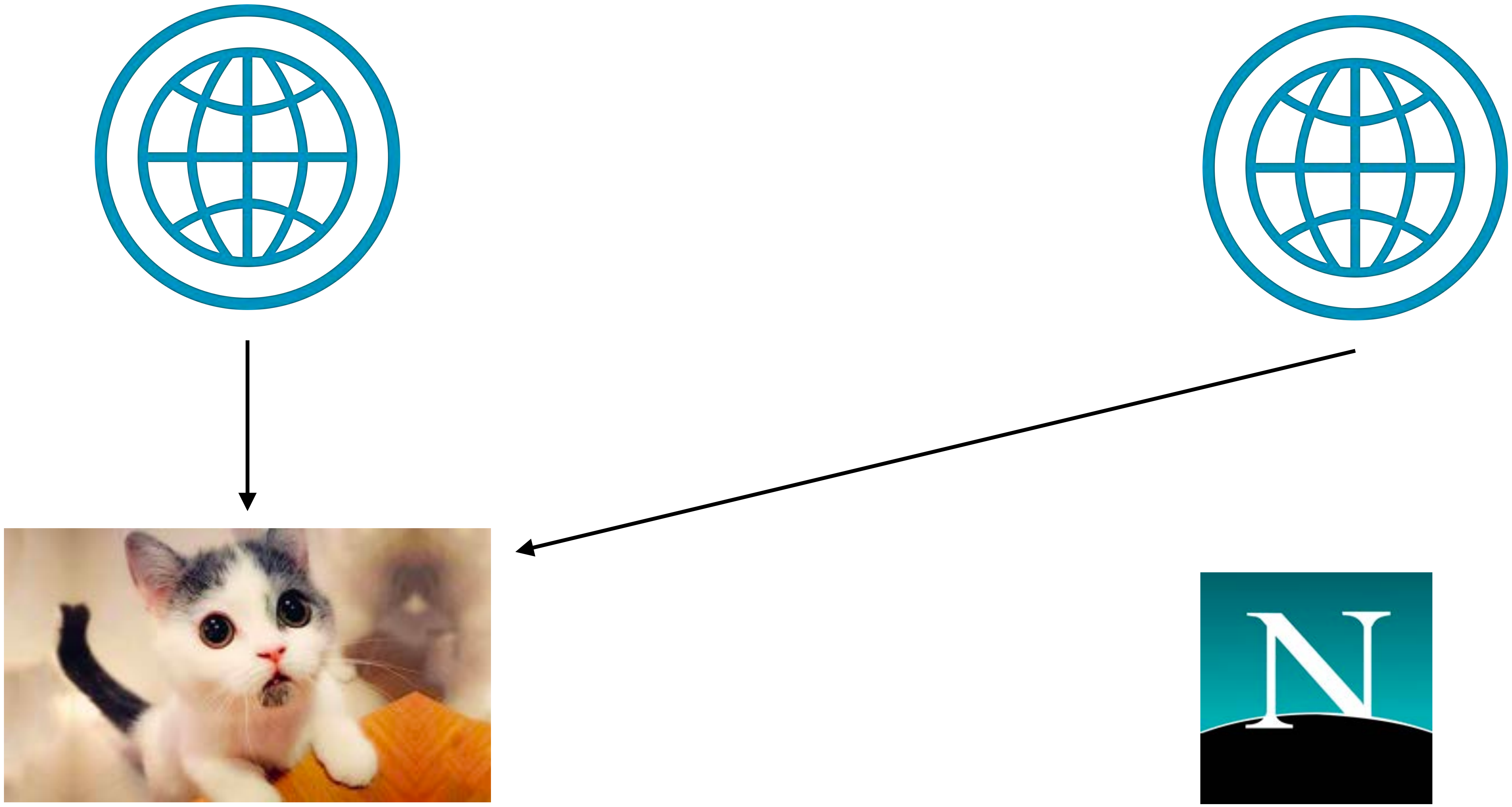
cat-cuties.com

kozy-kittens.com



cat-cuties.com

kozy-kittens.com



cat-cuties.com

kozy-kittens.com

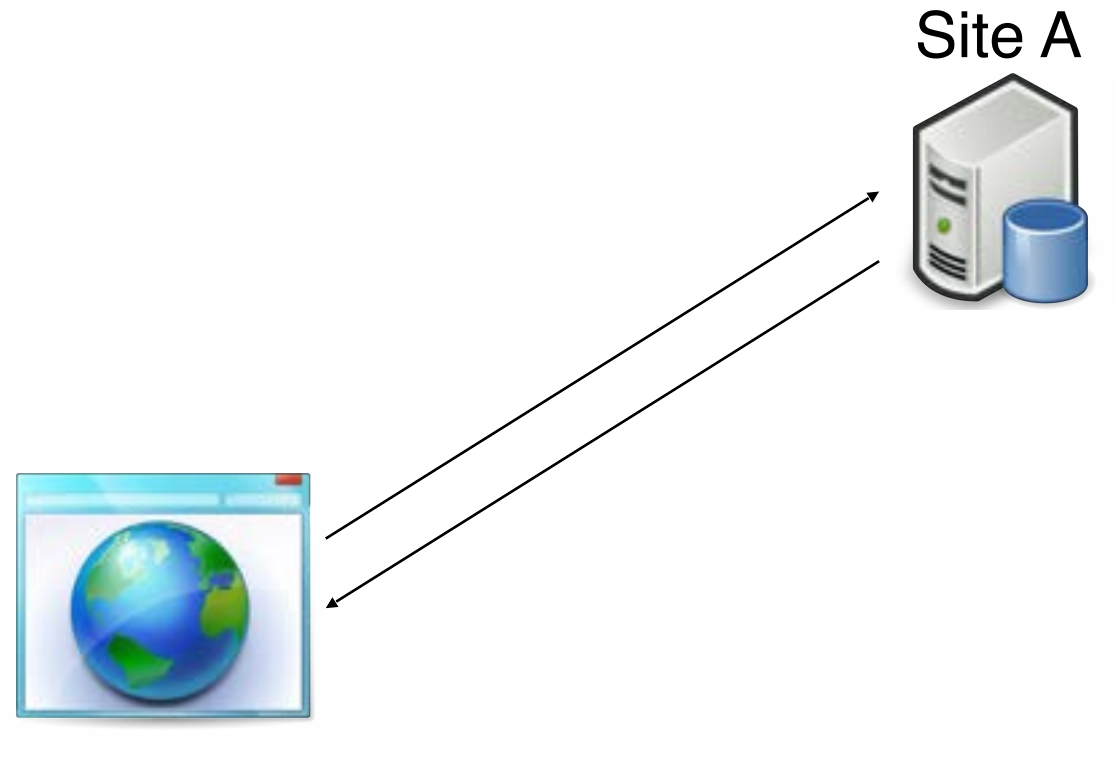
cookies, cookies everywhere…

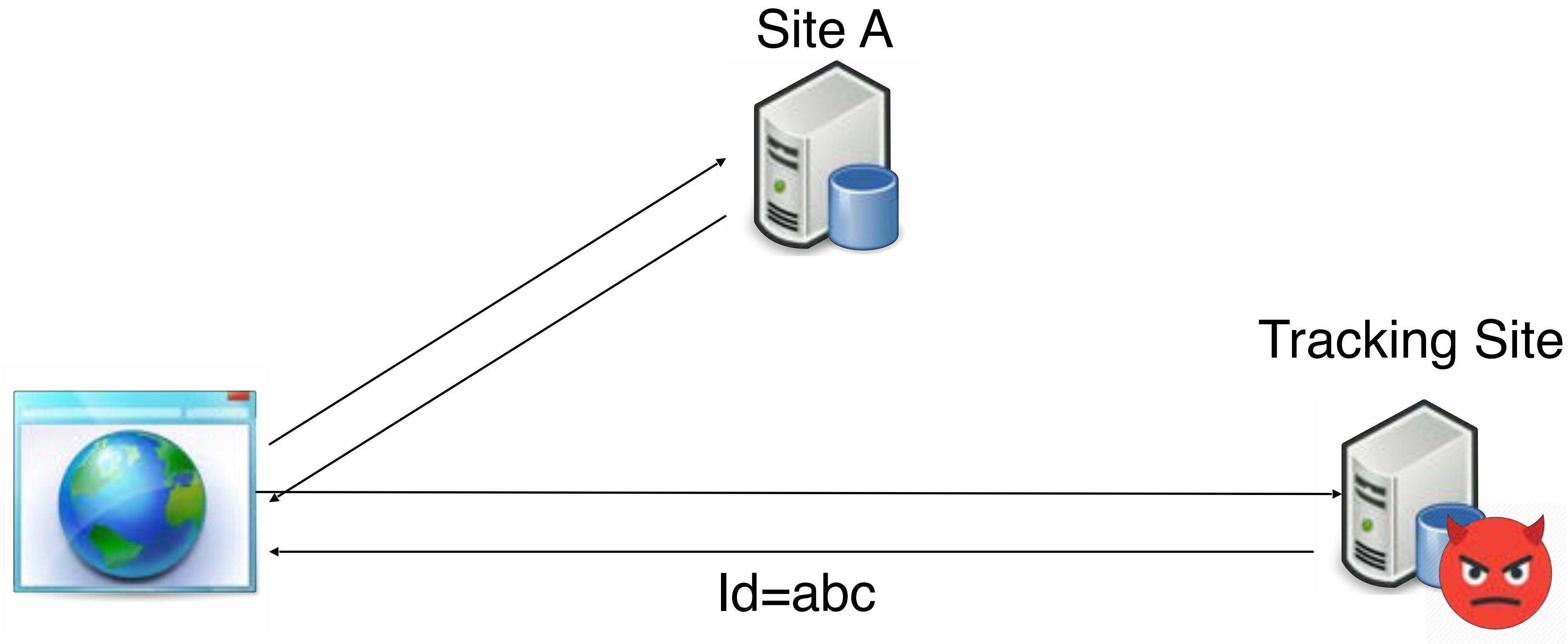
Cookies

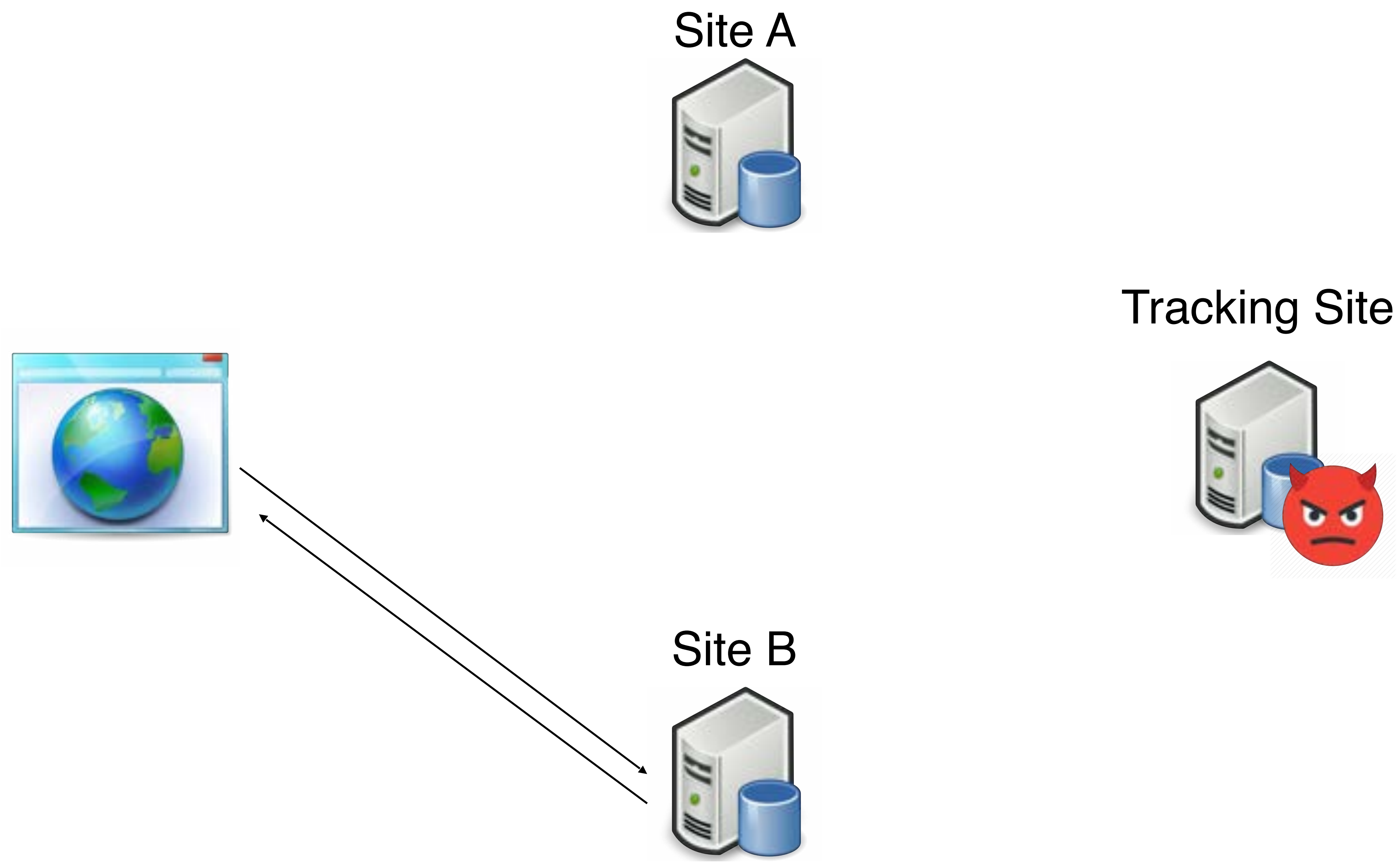
+ 3p Resources

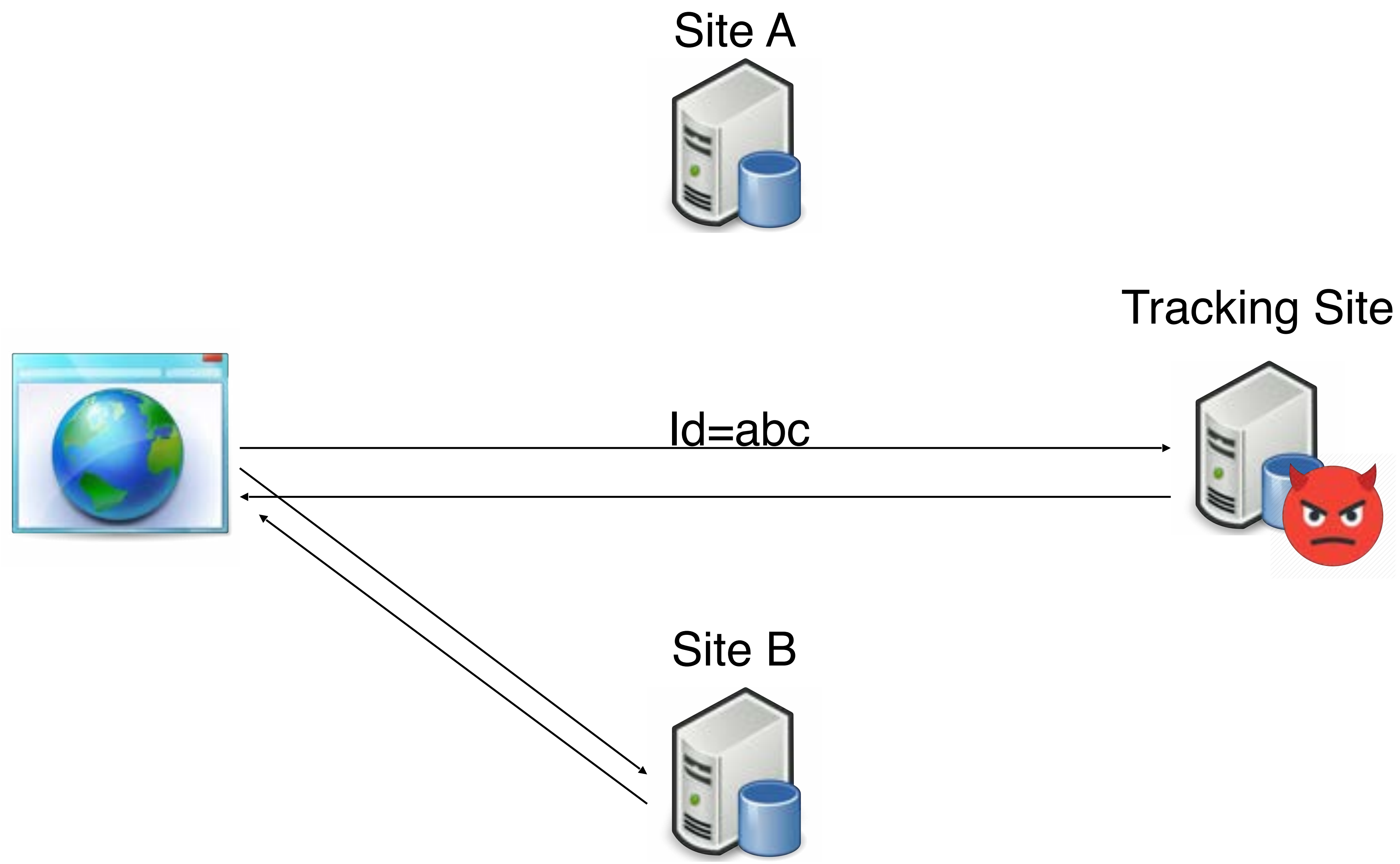
— — — — — — — —

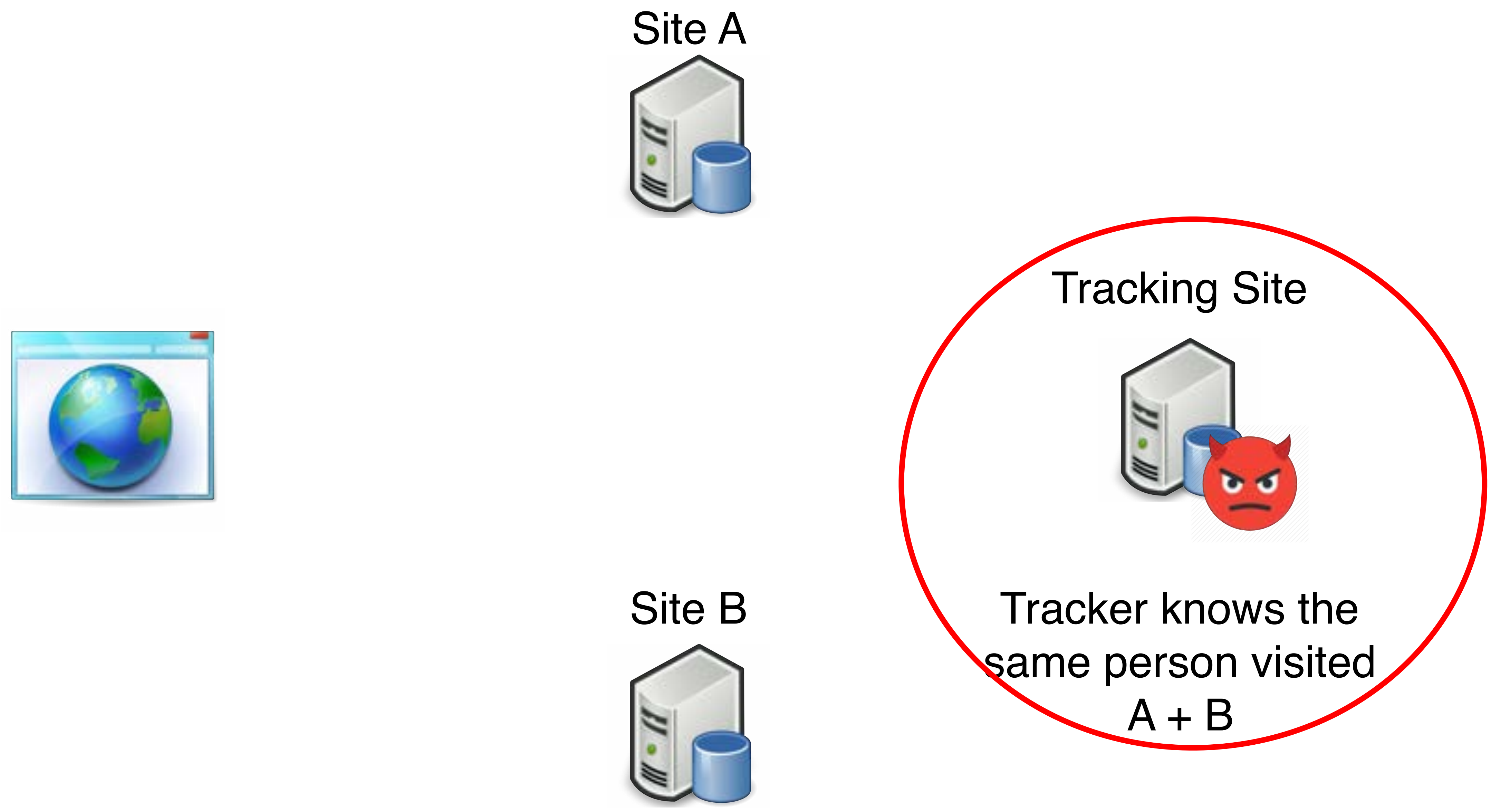
Tracking


Site A


Site A
Tracking Site
Id=abc


Site A
Tracking Site
Site B


Site A
Tracking Site
Id=abc
Site B



Site A

Tracking Site

Tracker knows the same person visited A + B

Site B

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

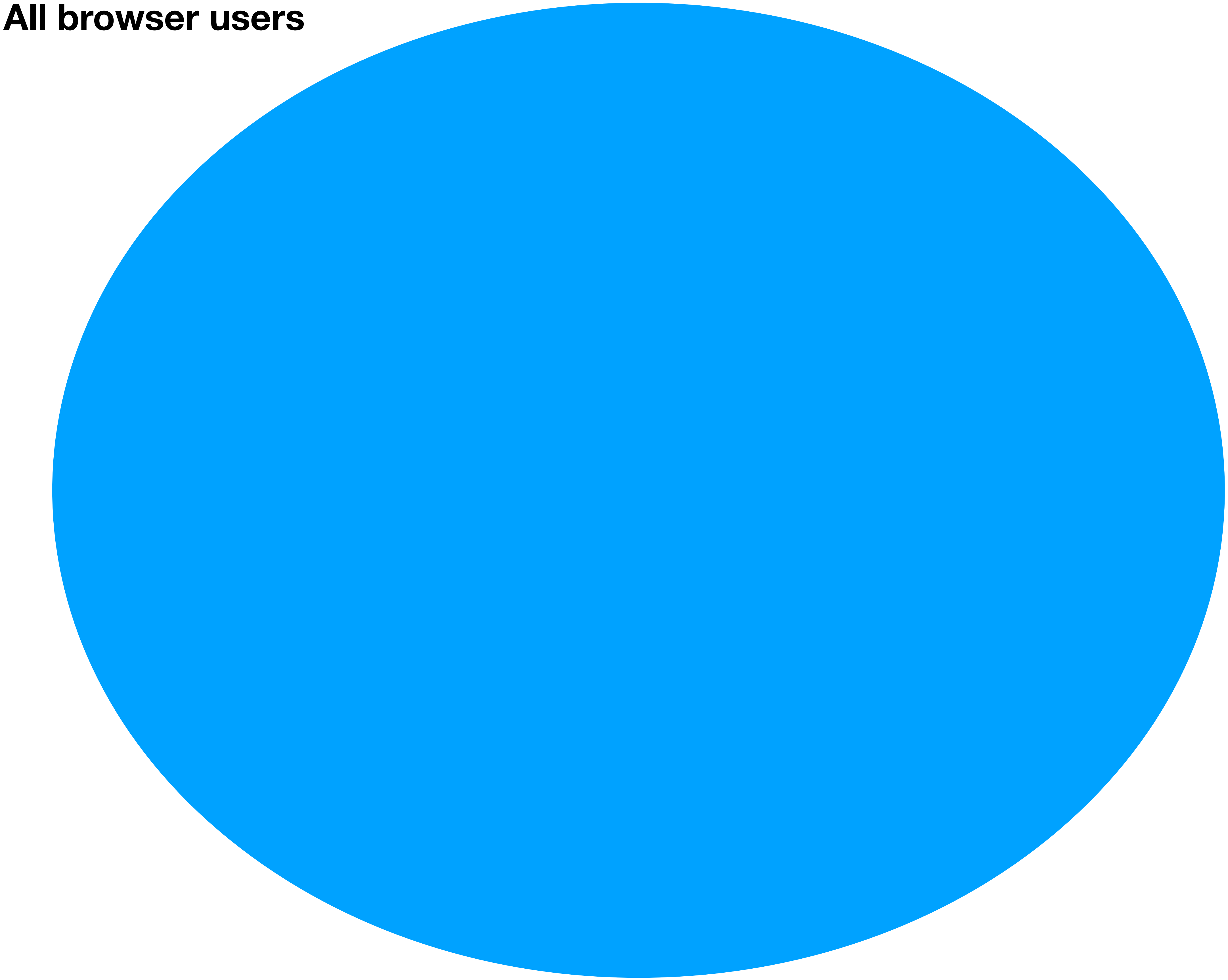
Fingerprinting, what’s diff?

- **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

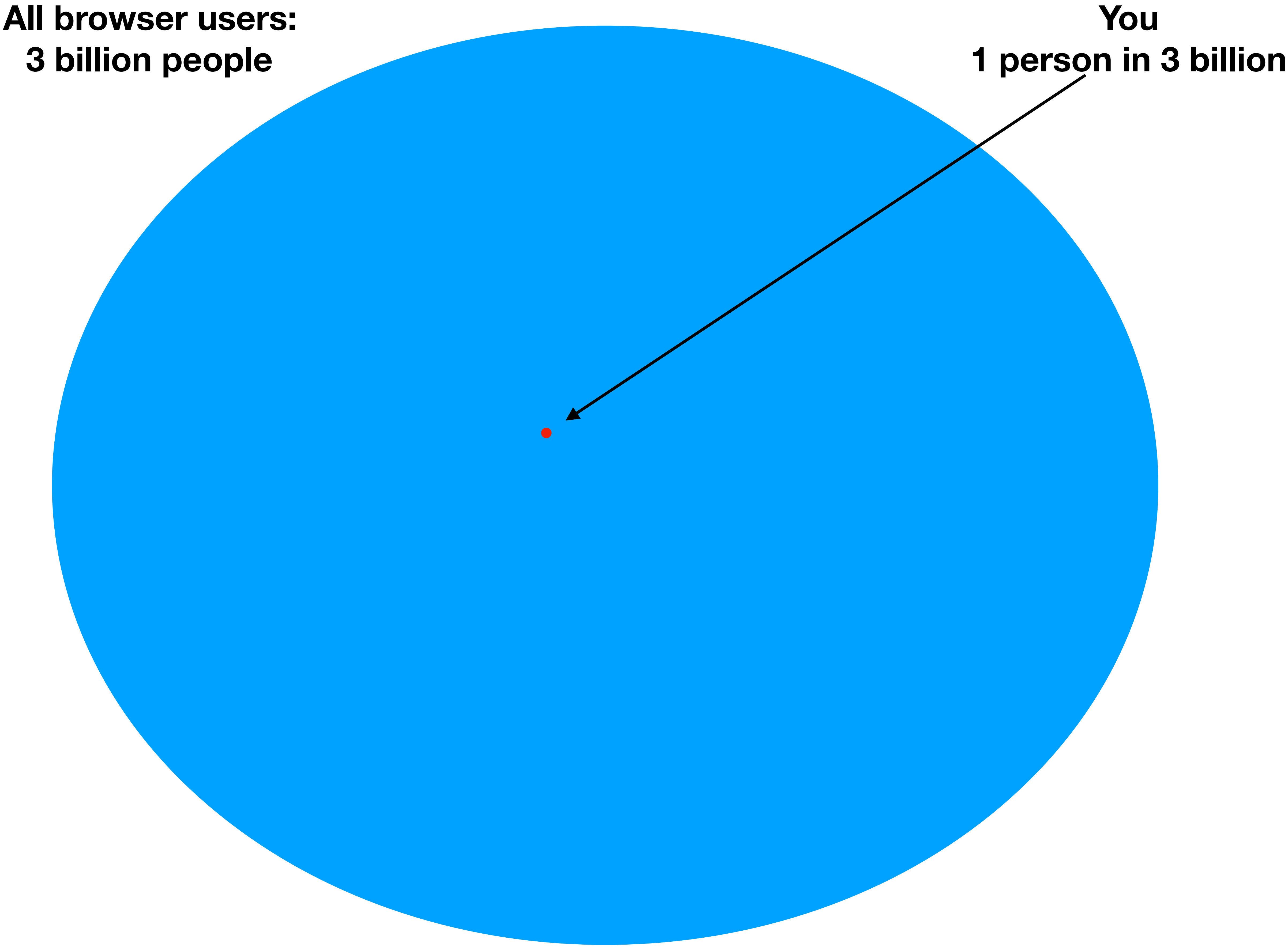
- **Fingerprinting / passive tracking**
  - Website finds things different about each visitor
  - That difference allows re-identification

Fingerprinting, how

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



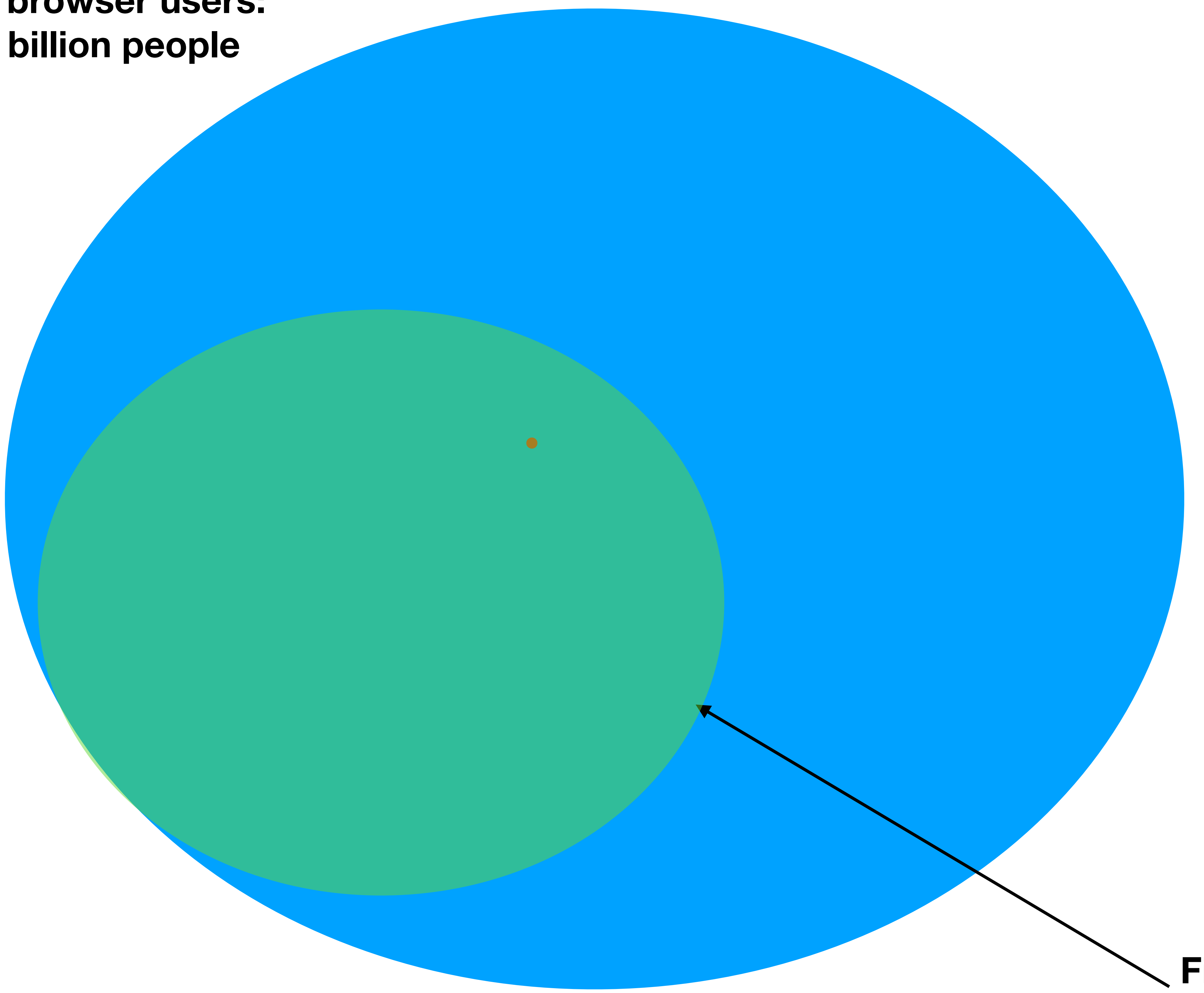
All browser users



All browser users:
3 billion people

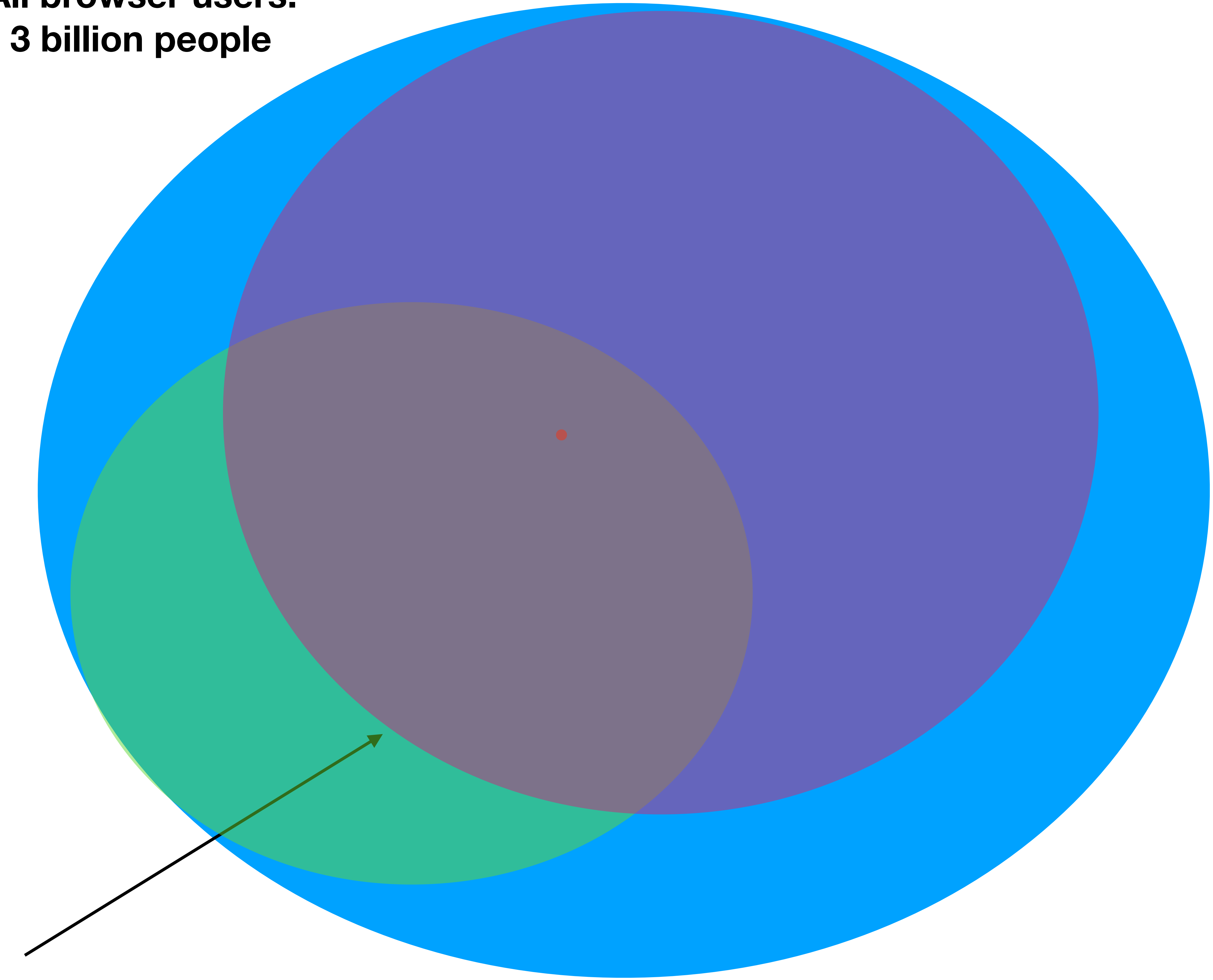
You
1 person in 3 billion

All browser users:
3 billion people

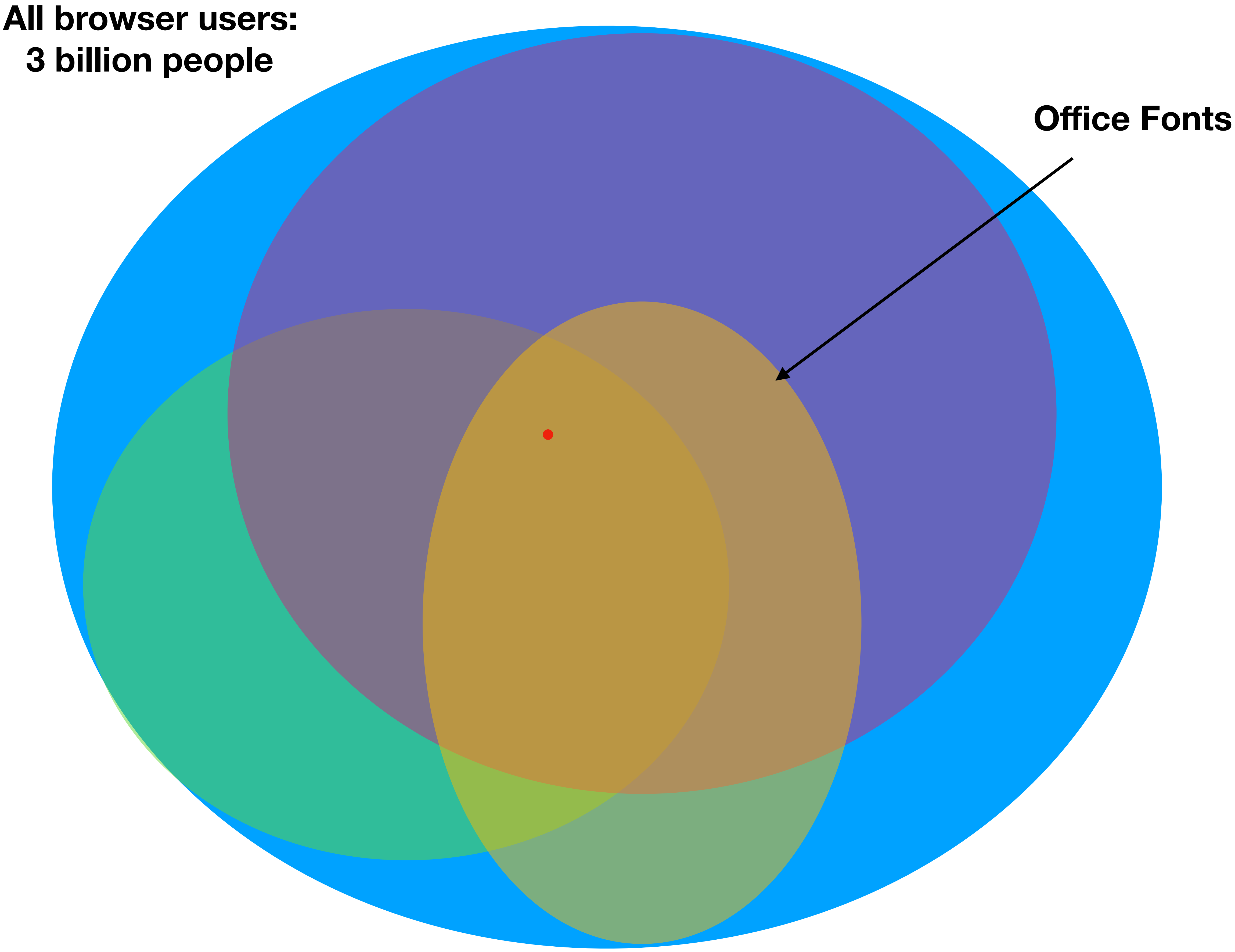


Firefox
Users

All browser users:
3 billion people

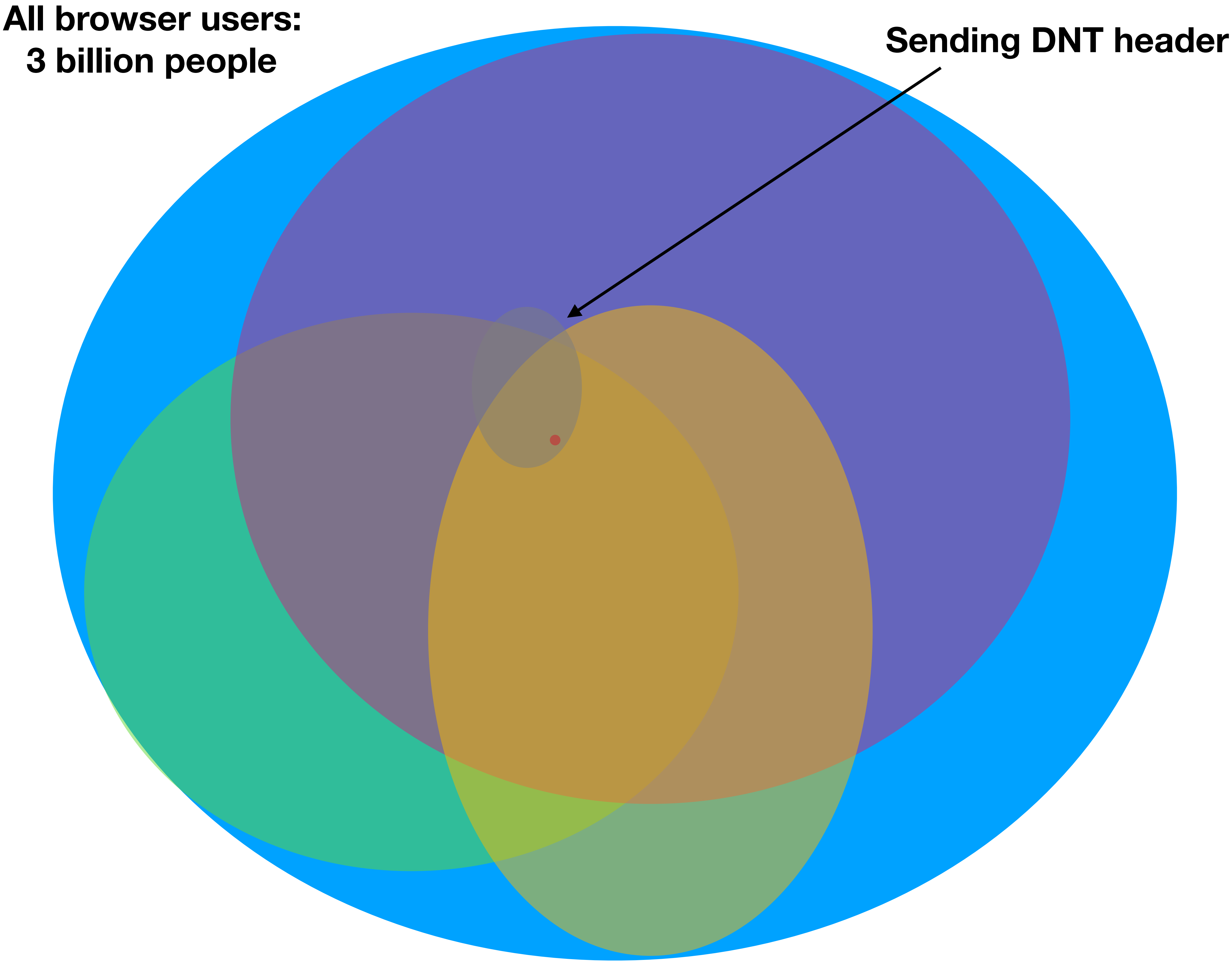


Windows users

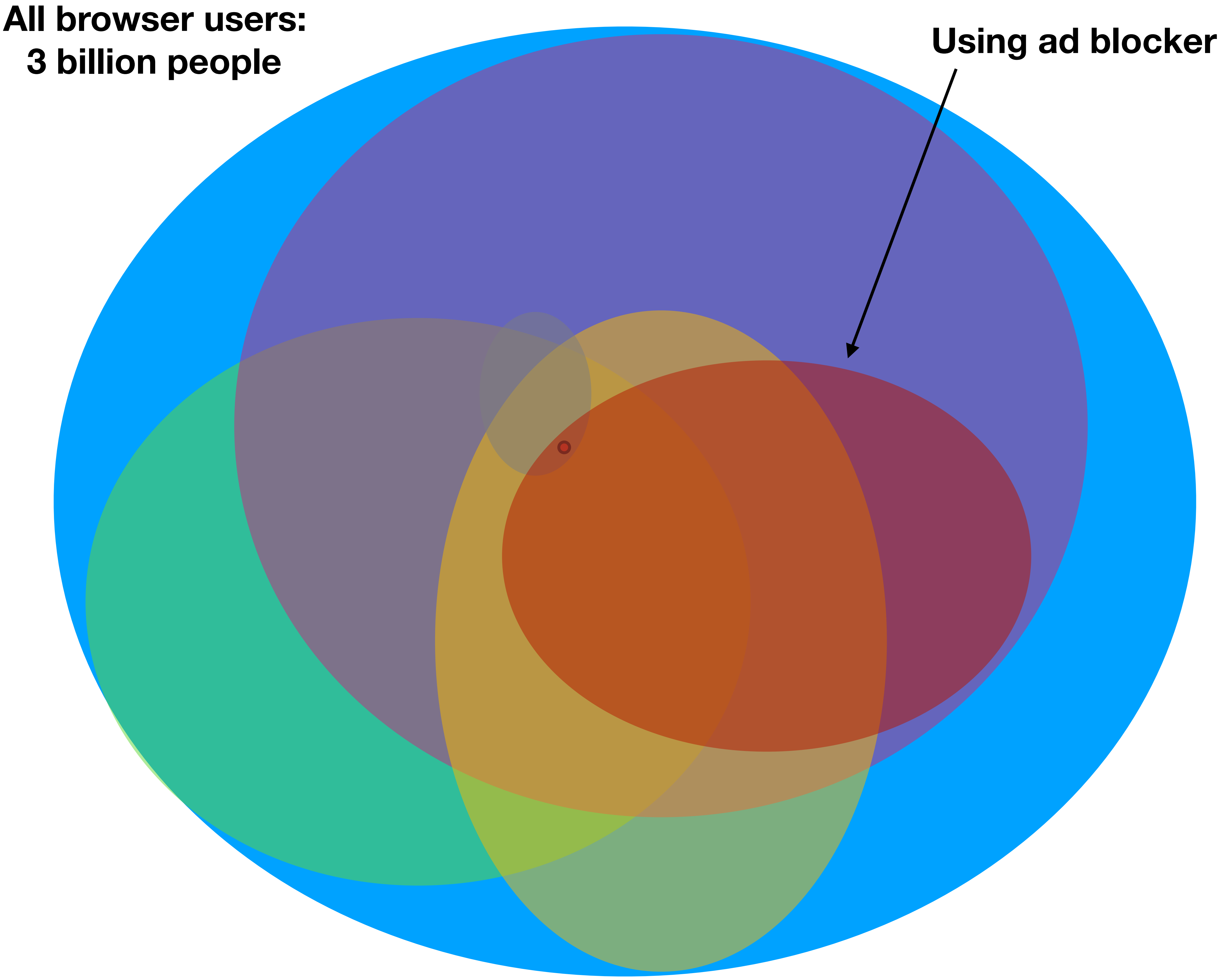


All browser users:
3 billion people

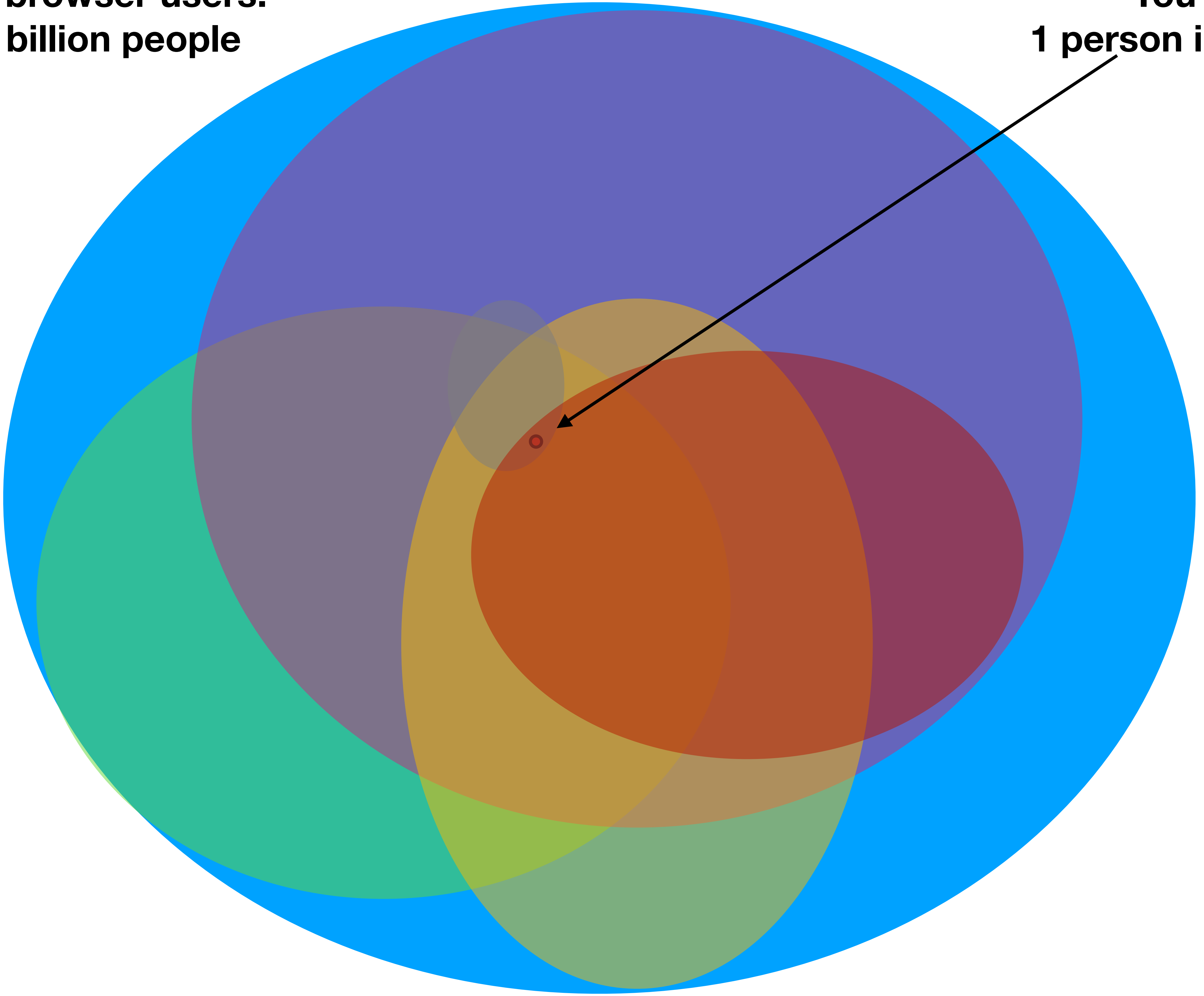
Office Fonts



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

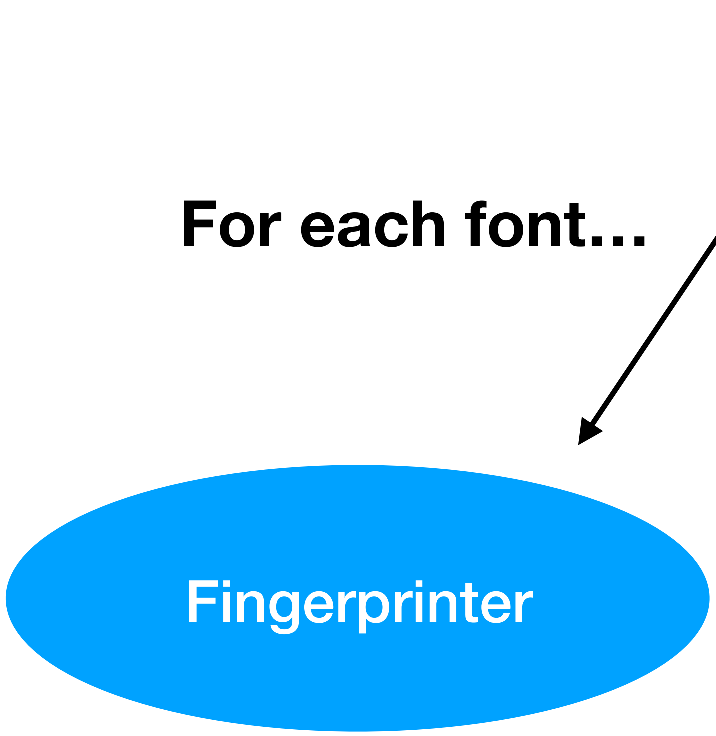
- **Easy to extract**
  - plugins
  - css + span + width

```
[‘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’…]

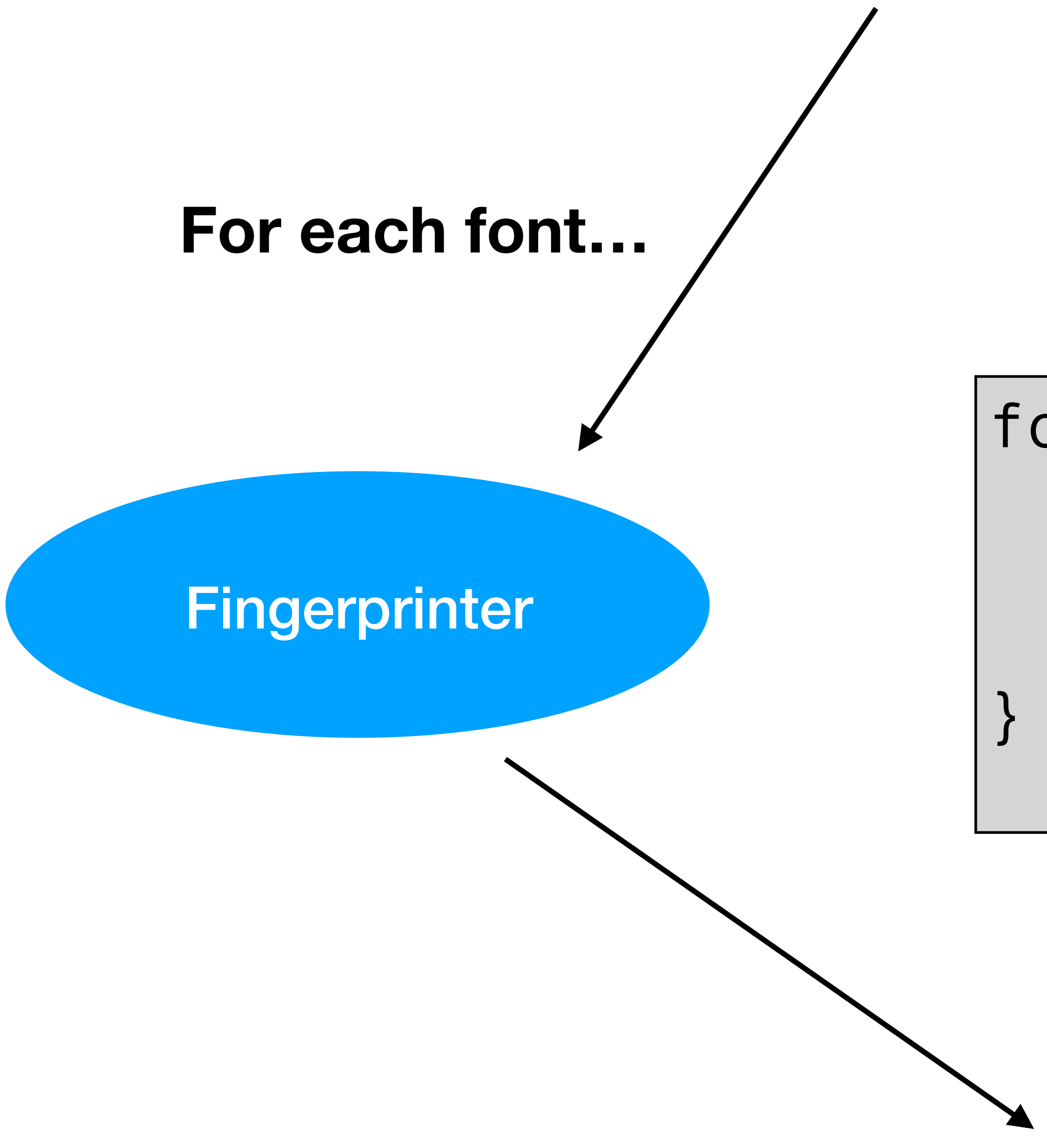


For each font…

Fingerprinter

```
<span>Example</span>
```

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



```
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>
```

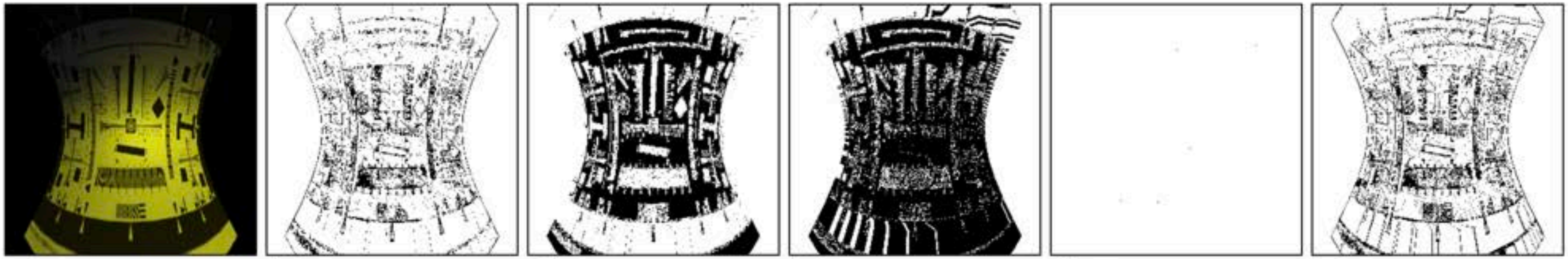
Canvas / WebGL

- **Pixel Perfect: Fingerprinting Canvas in HTML5**
  Keaton Mowery and Hovav Shacham

- **Drawling 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

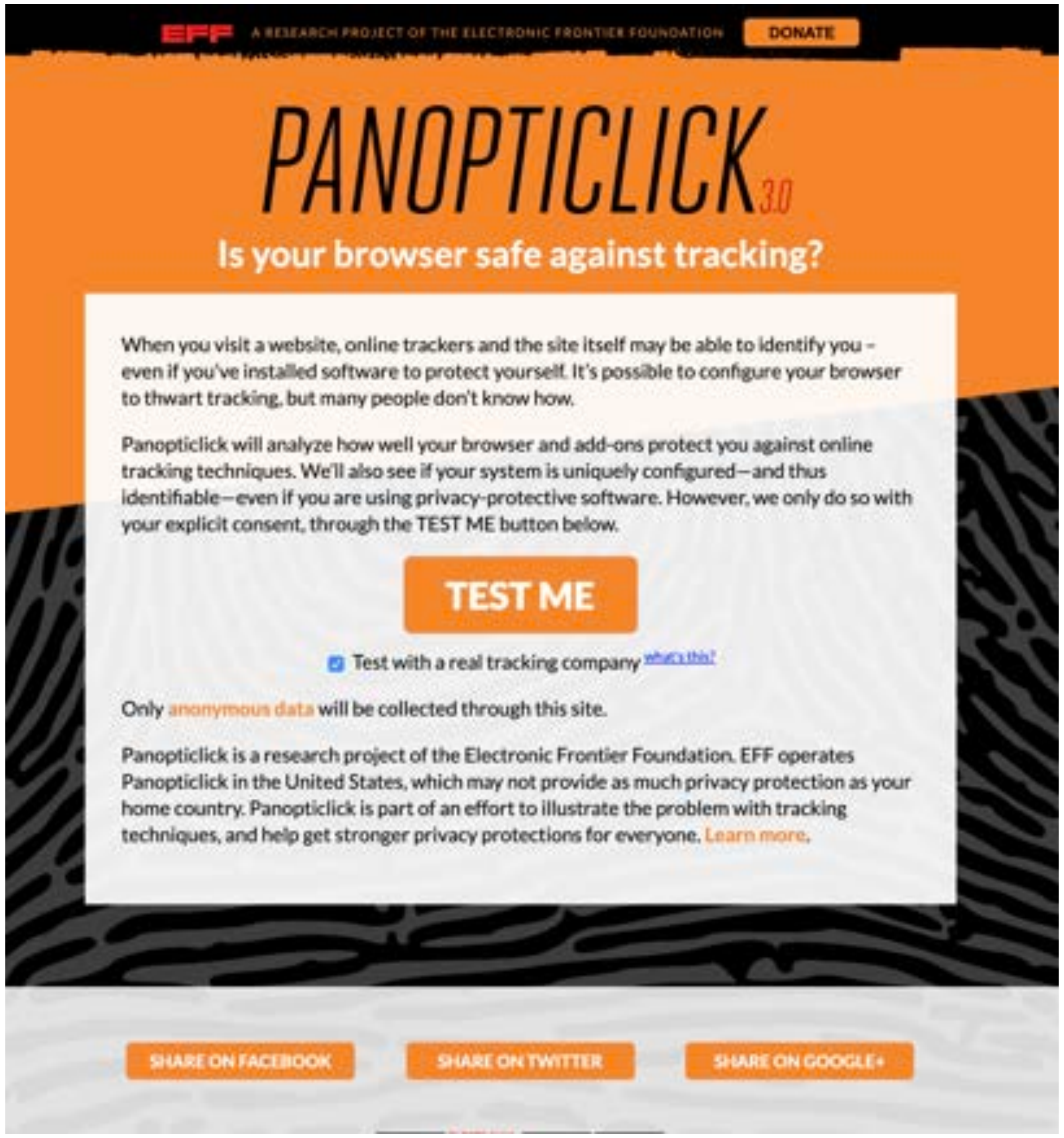
Height / Width

?

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



Is your browser safe against tracking?

When you visit a website, online trackers and the site itself may be able to identify you - even if you've installed software to protect yourself. It's possible to configure your browser to thwart tracking, but many people don't know how.

Panopticlick will analyze how well your browser and add-ons protect you against online tracking techniques. We'll also see if your system is uniquely configured—and thus identifiable—even if you are using privacy-protective software. However, we only do so with your explicit consent, through the TEST ME button below.

☑ Test with a real tracking company what's this?

Only anonymous data will be collected through this site.

Panopticlick is a research project of the Electronic Frontier Foundation. EFF operates Panopticlick in the United States, which may not provide as much privacy protection as your home country. Panopticlick is part of an effort to illustrate the problem with tracking techniques, and help get stronger privacy protections for everyone. Learn more.

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

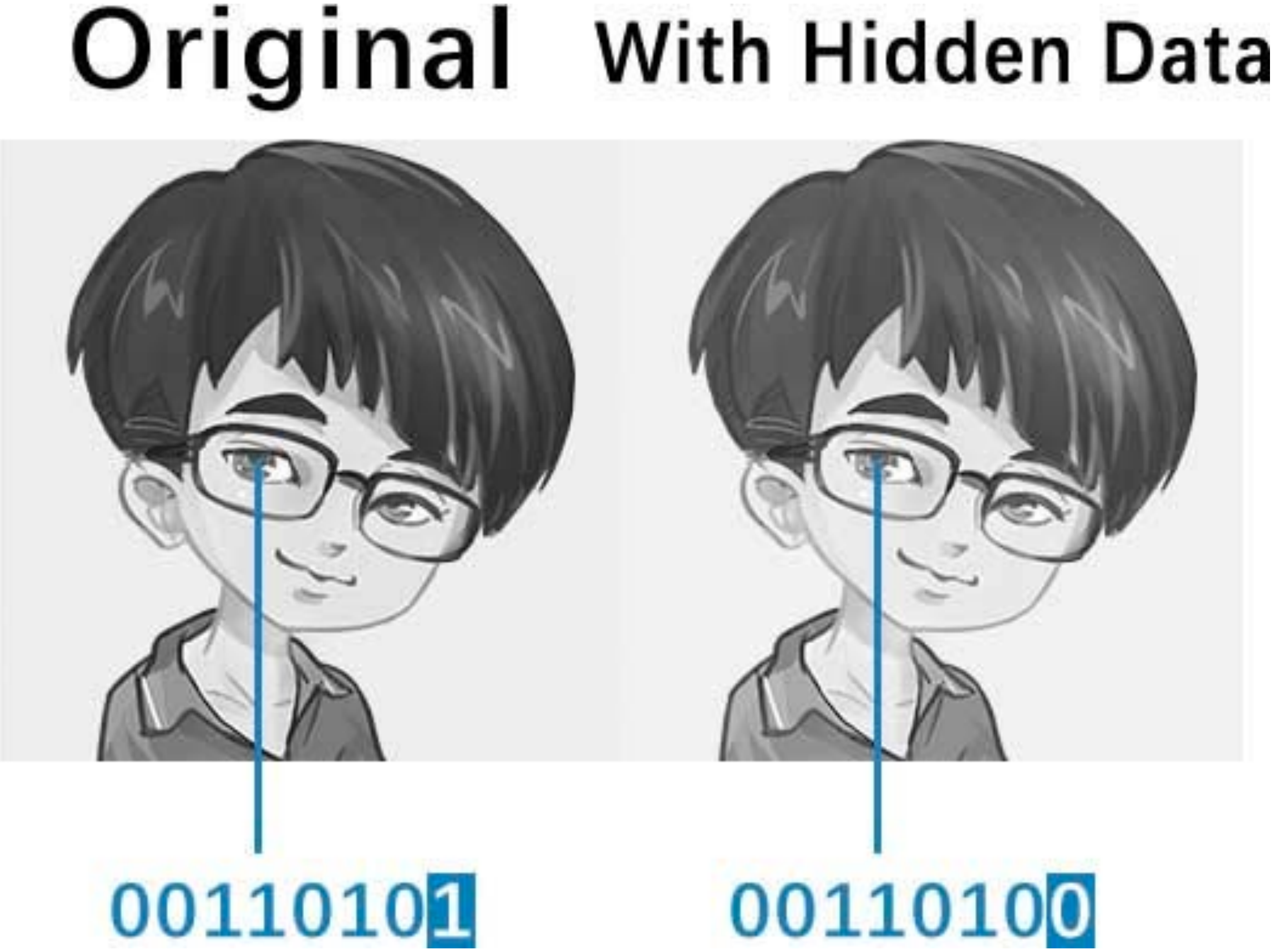
- Make every browser return the same value
- … or, most?
- Not that diff in practice from “removing”

Restrict access

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

Noise

- Stenography
- Make different every time



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 your the attacker
- How would you respond to those defenses…

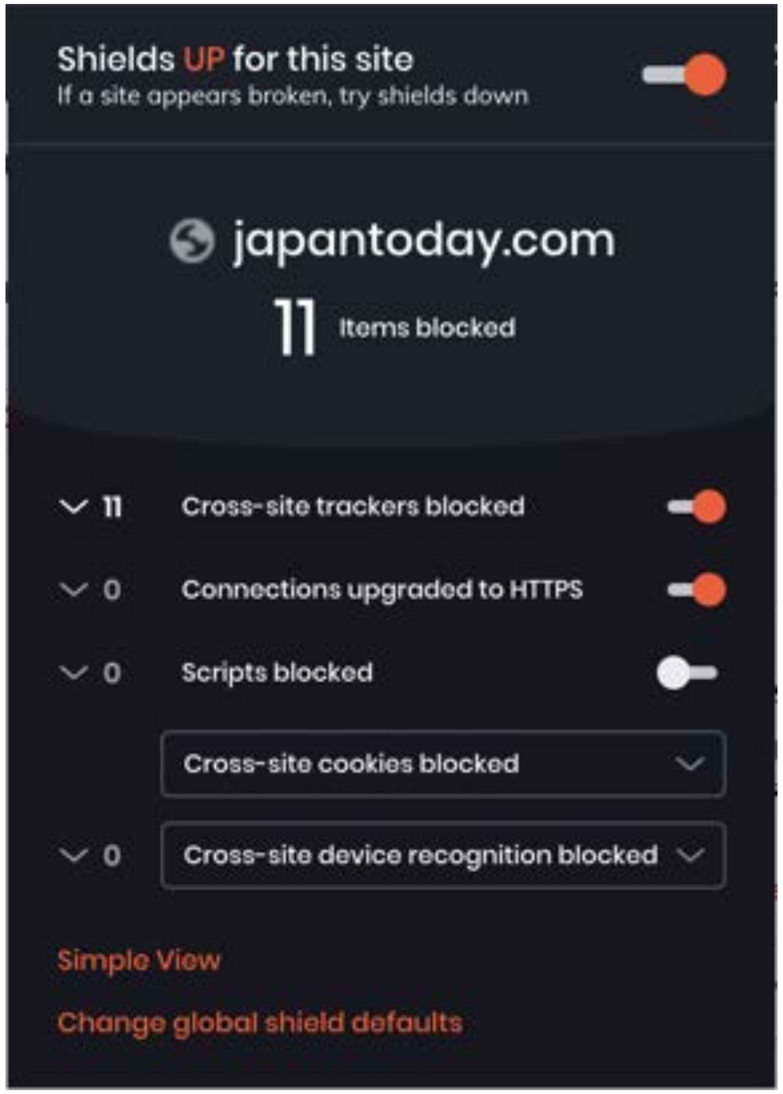
Fingerprint2 pt 4…

- Pretend your 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



Shields UP for this site
If a site appears broken, try shields down

japantoday.com

11 Items blocked

11 Cross-site trackers blocked

0 Connections upgraded to HTTPS

0 Scripts blocked

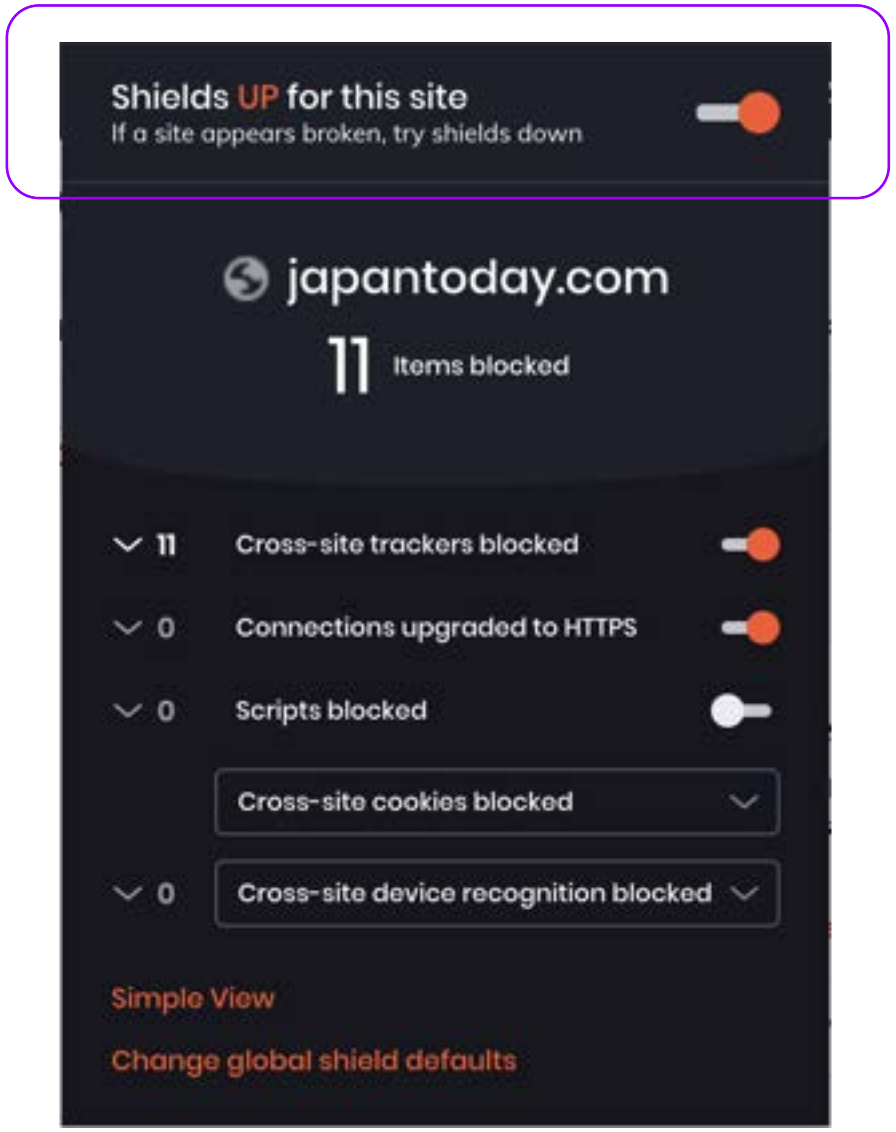
Cross-site cookies blocked

0 Cross-site device recognition blocked

Simple View

Change global shield defaults

Brave Privacy Protections



Shields UP for this site
If a site appears broken, try shields down

japantoday.com

11 Items blocked

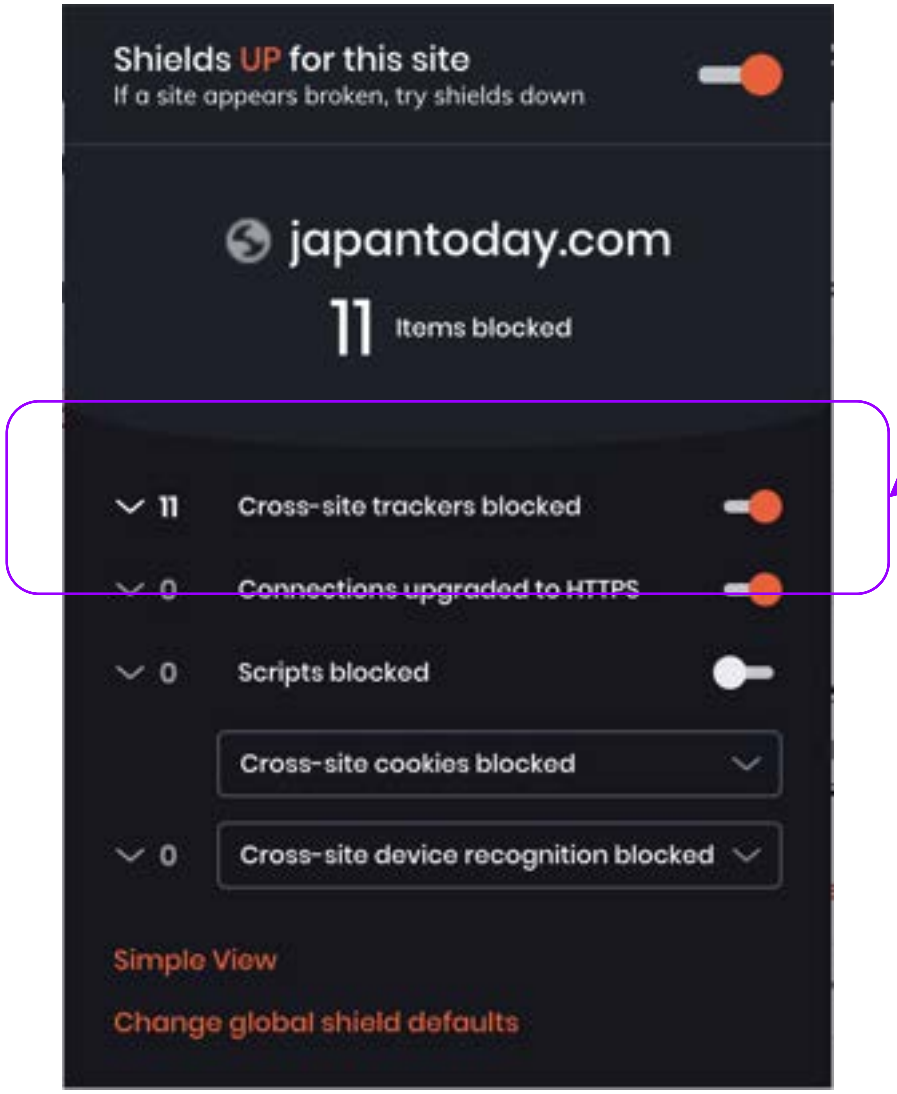
- 11 Cross-site trackers blocked
- 0 Connections upgraded to HTTPS
- 0 Scripts blocked
- Cross-site cookies blocked
- 0 Cross-site device recognition blocked

Simple View

Change global shield defaults

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

Brave Privacy Protections



Shields UP for this site
If a site appears broken, try shields down

japantoday.com
11 Items blocked

11 Cross-site trackers blocked

0 Connections upgraded to HTTPS

0 Scripts blocked

Cross-site cookies blocked

0 Cross-site device recognition blocked

Simple View

Change global shield defaults

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

Blocking Cross-Site Trackers in Brave

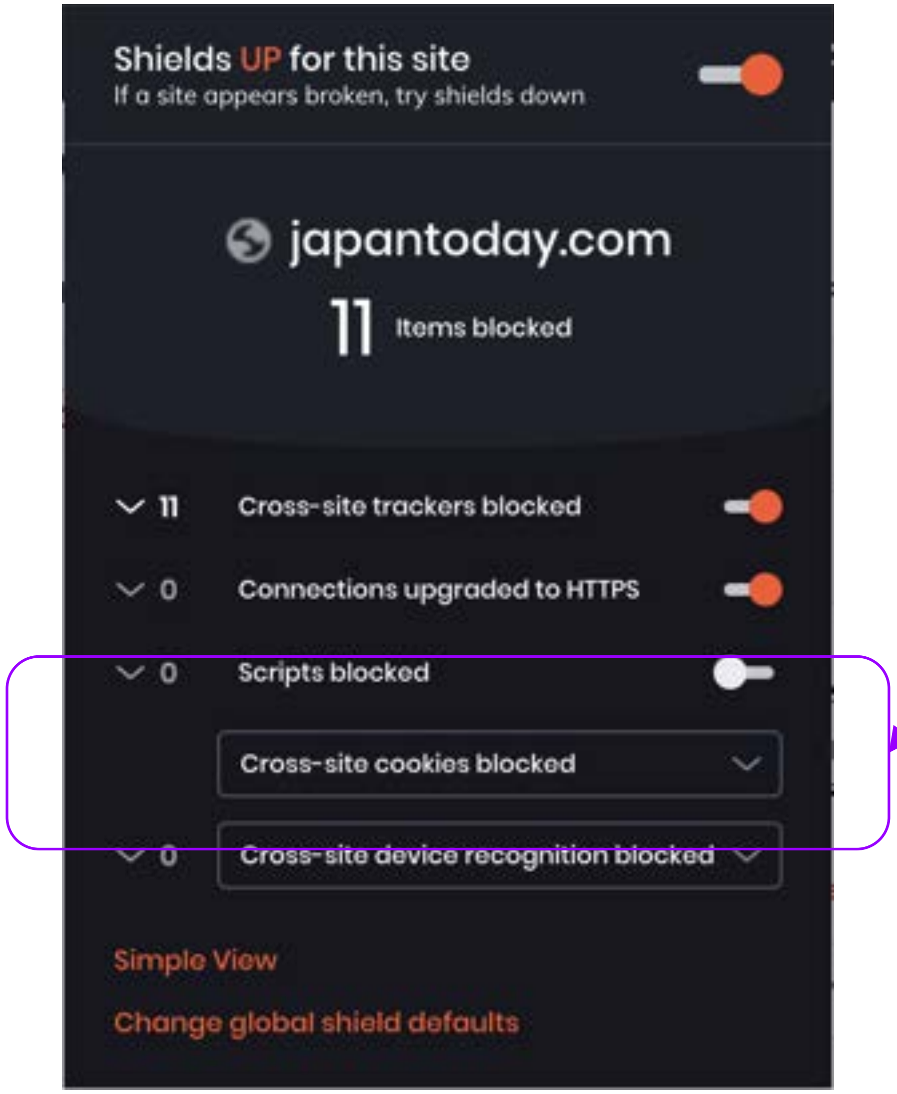
- **EasyList and EasyPrivacy**
  Used by AdBlock Plus, etc.

- **Disconnect**
  Used by Firefox, extensions

- **uBlock Origin**
  Excellent blocking extension

- **Brave generated**
  Open source, shared with community

Brave Privacy Protections



Shields UP for this site
If a site appears broken, try shields down

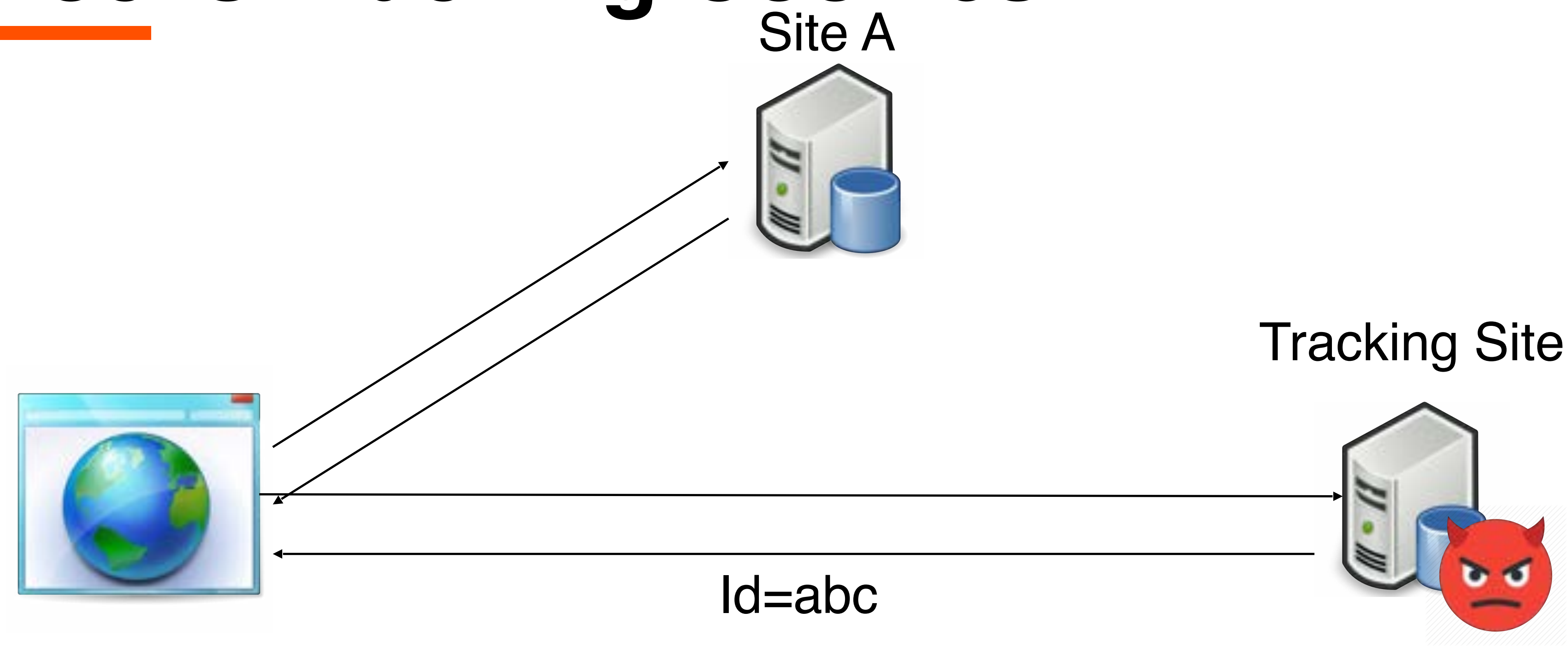
japantoday.com
11 Items blocked

- 11 Cross-site trackers blocked
- 0 Connections upgraded to HTTPS
- 0 Scripts blocked
- Cross-site cookies blocked
- 0 Cross-site device recognition blocked

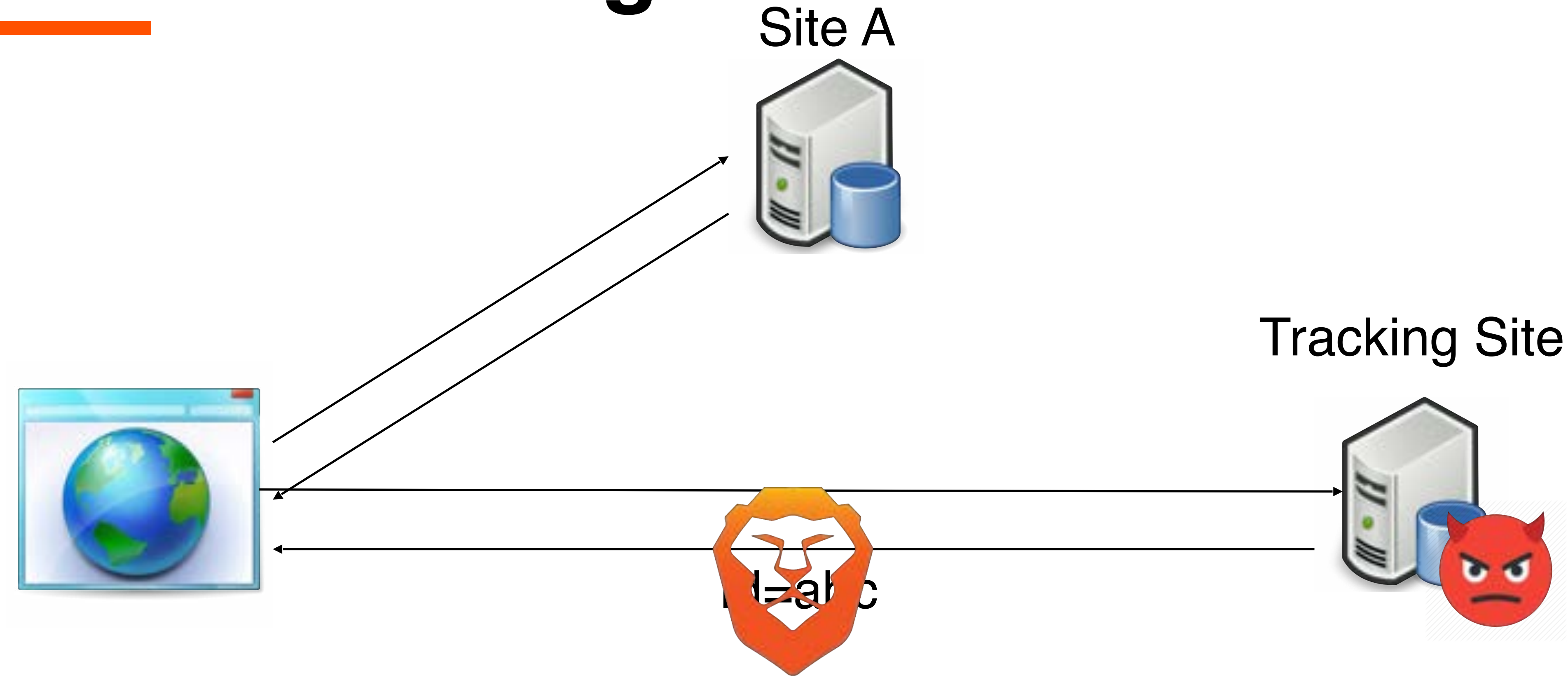
Simple View
Change global shield defaults

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

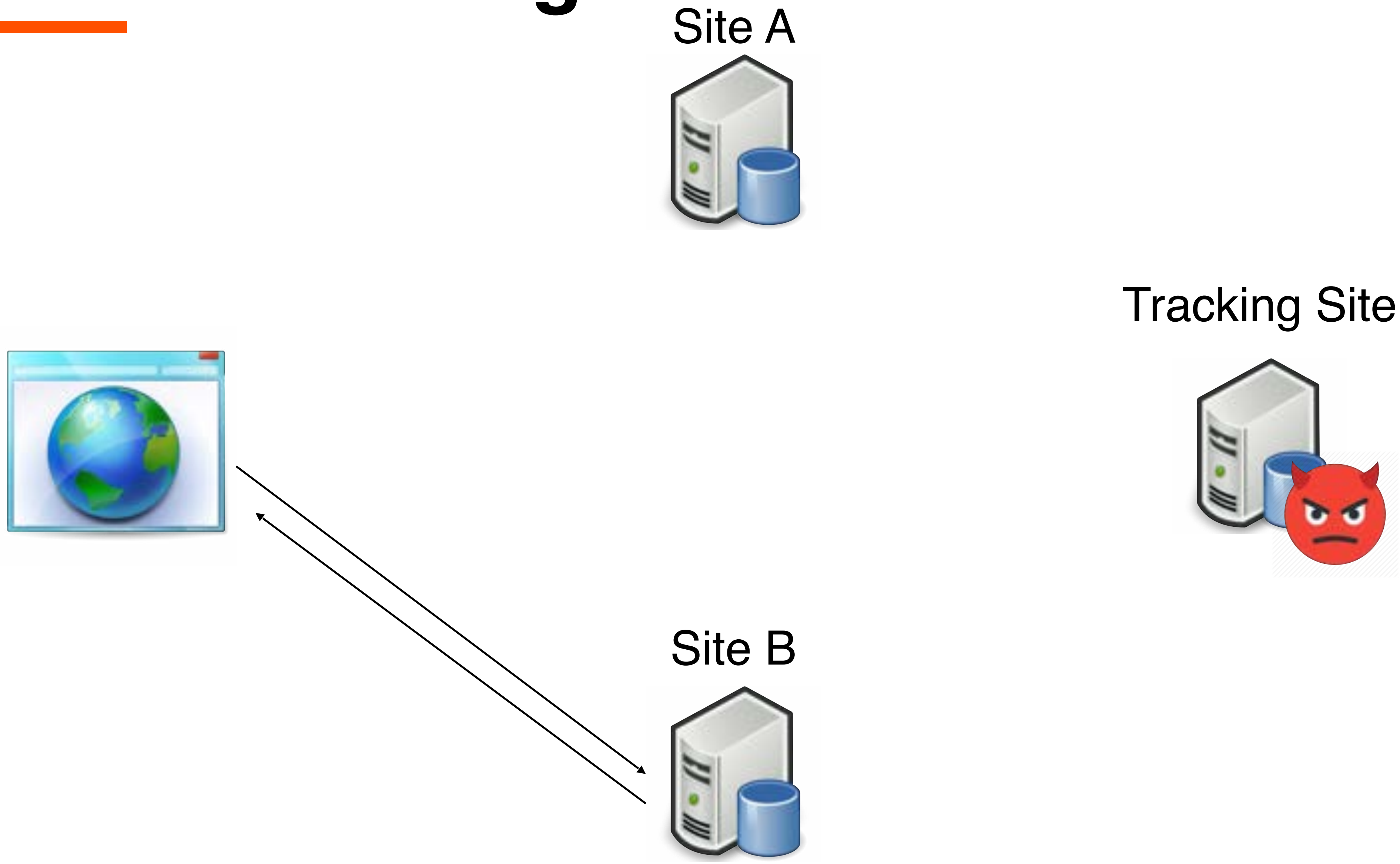
Brave Blocks Tracking Cookies



Brave Blocks Tracking Cookies



Brave Blocks Tracking Cookies

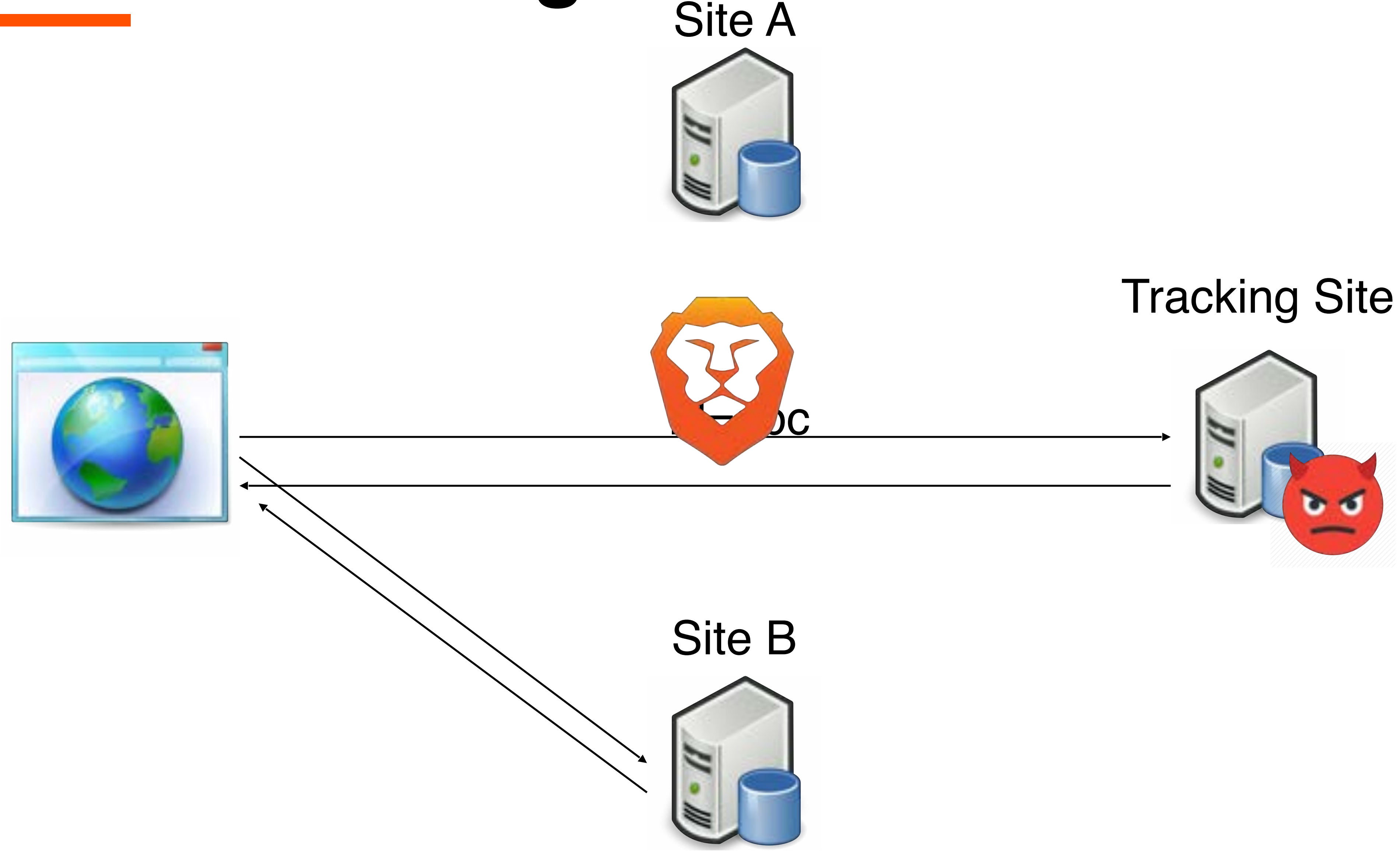


Site A

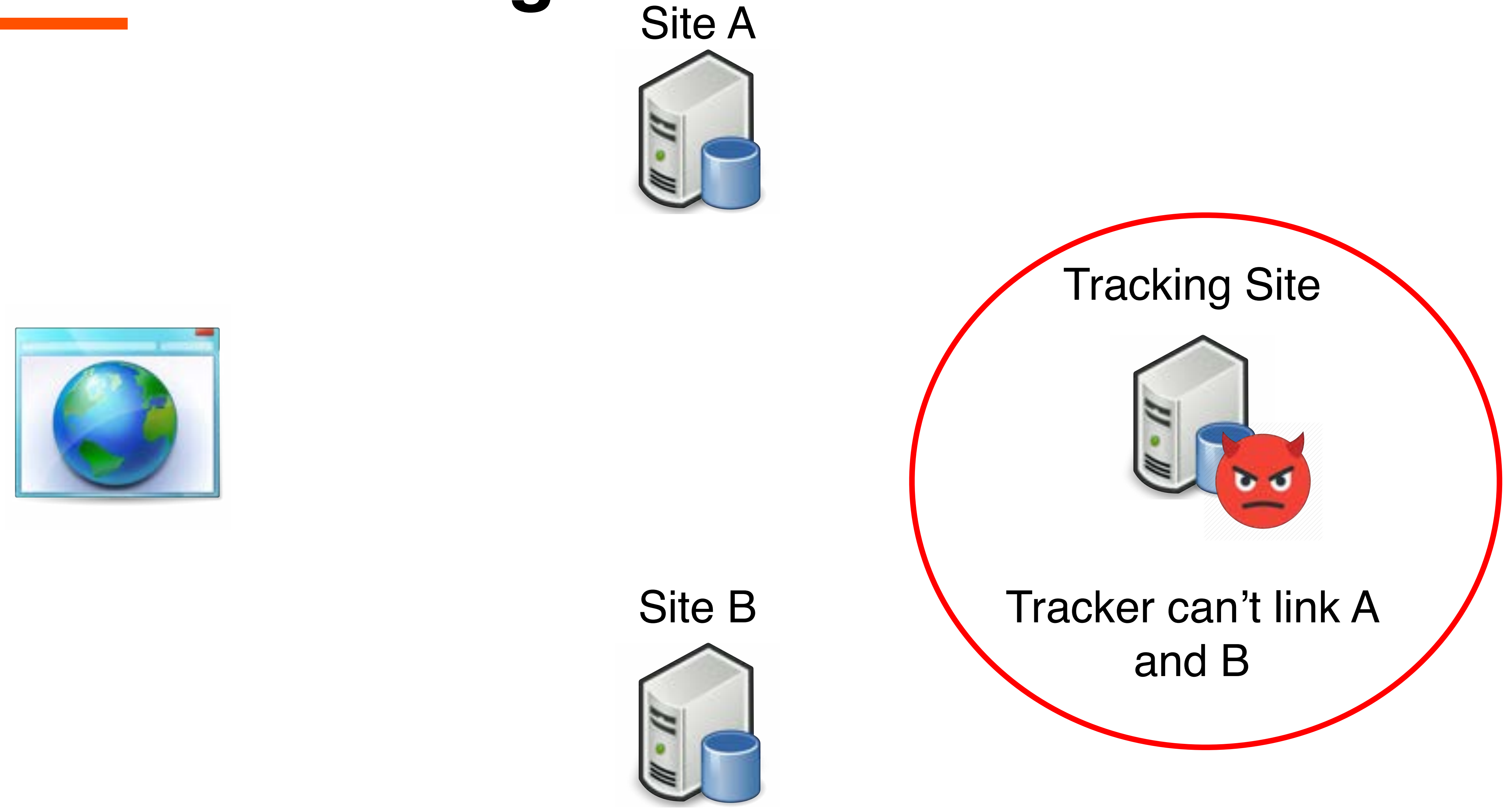
Tracking Site

Site B

Brave Blocks Tracking Cookies



Brave Blocks Tracking Cookies



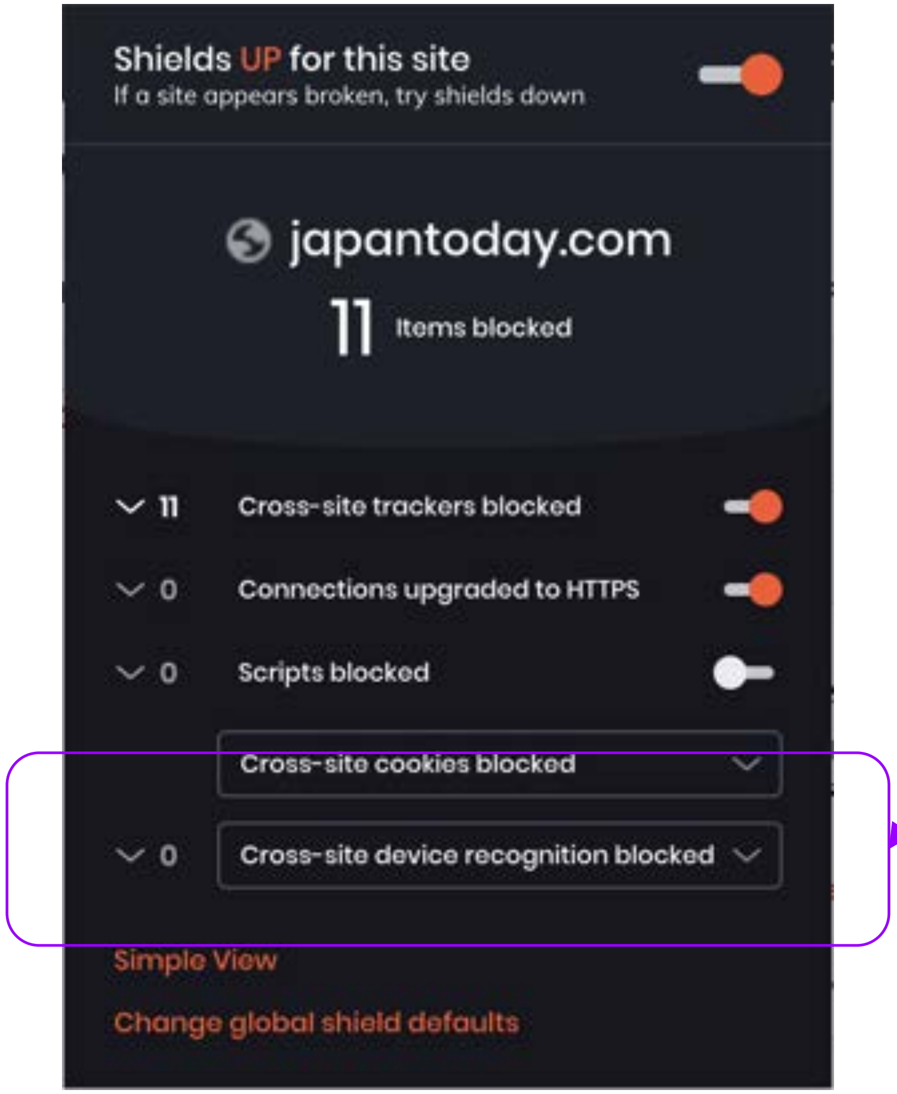
Site A

Tracking Site

Tracker can’t link A and B

Site B

Brave Privacy Protections



Shields UP for this site

If a site appears broken, try shields down

japantoday.com

11 Items blocked

11 Cross-site trackers blocked

0 Connections upgraded to HTTPS

0 Scripts blocked

Cross-site cookies blocked

0 Cross-site device recognition blocked

Simple View

Change global shield defaults

- 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
  @pes10k

- Questions?
  - Standards work?
  - Privacy jobs?
  - Brave business model
  - BAT / Block chain
  - Anything else?