

Online Tracking, What Can Be Done About it, and Who's Doing it

Pete Snyder

Senior Privacy Researcher, Director of Privacy

pes@brave.com



Hi, I'm Pete 🙌

- **Grew up in Chicago**
...actual Chicago
- **Law school -> freelance web stuff**
Started: Anchorage, AK
Ended: Judge Judy Show invitation
- University of Illinois at Chicago



Me at Brave

- **Research at Brave**
...privacy, blocking, reliability
- **Co-Chair of PING**
Privacy committee on W3C
- **Research <-> Engineering**
Web compat, filter lists, etc.
- **Academic <-> Industry**
Collaborations



Brave in a Slide

- **Privacy focused**
- **Alternative web funding model**
Fix incentive problems
- **Research + Engineering**
- **Not just a browser**
 - search.brave.com
 - talk.brave.com
 - VPN
 - more coming...



Overview

- **Why Privacy Matters**
A sloppy manifesto
- **Defining Tracking**
Abstracting the problem
- **Tracking in Practice**
Methods and defenses
- **Privacy Beyond Tracking**
Other issues and concerns

Overview

- **Why Privacy Matters**
A sloppy manifesto
- **Defining Tracking**
Abstracting the problem
- **Tracking in Practice**
Methods and defenses
- **Privacy Beyond Tracking**
Other issues and concerns



Why Does Tracking Exist?





TAYLOR... big audition

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.

Metts star Taylor said: "We must put the World Cup behind us — 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 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. ENGLAND (in plus boxes): Hales, Roy, Taylor (capt), Eoin, Ansari, Billings (wk), Broad, Gregory, Willey, Vince.

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 610-8 against Surrey at The Oval.

Kent's Geoffrey 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 116. KP was eight not out as Surrey trailed by 175 runs in their second innings.

Lee: Oui will return

By JOHNNY 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 NO'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."



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 FIC — Future England Captain.

Everyone expects it to happen and I've little doubt he will lead England at some point. But I hope and pray it doesn't happen for at least five years, by which time he will be only 28.

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 feign gravitas. That simply is not Joe.

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

Just let Joe Root bat at No6 and score hundred after hundred. He can be England's Steve Waugh.

I don't think about moving him up the order, either.

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

this angelic face and looks as though butter wouldn't melt in his mouth. He's at his best when chatting away, taking the mickey and behaving like your annoying little brother.

He doesn't really sledge. It would be like being sledged by a baby because of the way 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. You don't score eight international centuries in the past 14 months without being a tough cookie.

The key to Rooty's success is he discovered the secret of Test cricket very early.

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

this angelic face and looks as though butter wouldn't melt in his mouth. He's at his best when chatting away, taking the mickey and behaving like your annoying little brother.

He doesn't really sledge. It would be like being sledged by a baby because of the way 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. You don't score eight international centuries in the past 14 months without being a tough cookie.

The key to Rooty's success is he discovered the secret of Test cricket very early.

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

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

The Seagulls supremo placed £1.15m on himself to finish the Brighton Marathon in no more than 3hr 45 min — only to cross the line four minutes and 38 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.

Reporters were gathered to interview Gareth Barry when the subtle hints of team-mate Ross Barkley inevitably surfaced soving as he is the ONLY interesting topic of conversation at Goodison Park.

As soon as Barkley's name was mentioned, the club's subtle press officer came out with an outrageously staged cough — as in, be careful, here mate, tricky subject coming up!

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

Ooh, suits you Shaun

SHAUN MURPHY's garish suits have been downing fans, TV crews and players at snooker's world championships.

That spokesman for tournament sponsors Betfred, Mark "Shaun" Pearson, told VTD: "Every time we sponsor a tournament we give a prize for the best dressed nag, taking into account colour, condition and colours. It's with Shaun."

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

A Parker can cut it

SOMETHING for the weekend, sir?

Traditional barber's shops would always offer extras to gentlemen to keep them safe while enjoying the company of others on a Saturday night.

The latest marketing trend — "pop-up" shop and this one in South West London offered customers the chance to have their hair cut in the style of the captain Scott Fulham.

Let's be honest, Those Fulham supporters have more chance of getting a s*x than seeing their team win on Saturday.

WORLD SNOOKER



BAD TABLE MANNERS... Ronnie puts himself down

CHALK OF SHAME

O'Sullivan in dust-up

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.

The official should have called a foul and awarded Bingham seven points, but the Rocket was allowed to continue his break and won the fifth frame to lead 3-2.

Rule 3 (d) states a seven-point penalty will be awarded if a player "uses any object to measure pips or distance".

Former world champion Ken Doherty said: "You are not allowed to put chalk on the table because you are using it as a tool to measure the ball."

"That is exactly what Ronnie has done. Stuart Bingham was looking at him and should really be aware. If he had more knowledge of

JUDD HEA-DING THROUGH

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

Pep gets Klopped

From ANTONY KASTRIMAKIS

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.

Osaka 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 £9m a year merely to be "in association with" the trophy FA Cup — ended their three-year

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

Lawrie McMenamy, who guided Second Division Southampton to the Premier League, said: "I would have thought there was enough

money circulating in football in TV rights to avoid this Football Cup 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 over 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 £30m-a-year

Dubai-based Emirates — sponsors current Cup holders Arsenal's kit and made their move announcing a £30m-a-year relationship with the FA. An FA spokesman admitted: "We continue to have discussions with a number of parties about FA Cup partner opportunities."



BEEN READING THE GOSSIP COLUMNS THIS MORNING?

—RECLAIM YOUR MANLINESS—

LIMITED EDITION

• SAUSAGE & BACON SANDWICH •



Served before 10.30am. From 29th April until 9th June 2015. Subject to availability. © McDonald's 2015





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:



Chicago Tribune: Chicago news, x

chicagotribune.com

☆ | 🛡️ | 👤 | ⋮

☰ SECTIONS 🔍 SEARCH

NEWSPAPER 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

TOP LOCAL
NEWS SOURCE

OCTOBER 16, 2019

Chicago Tribune

\$2 FOR
20 WEEKS
ENDS 11/4

☁️ 51°F 🗺️

BREAKING NEWS

SPORTS

BUSINESS

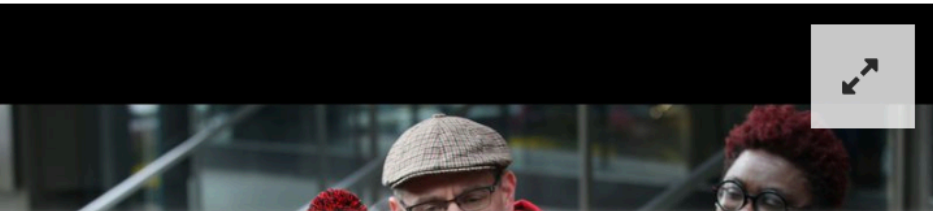
POLITICS

OPINION

ENTERTAINMENT

ADVERTISEMENT

CPS STRIKE IS ON



CPS strike is officially on as teachers union, Chicago

MORE CPS STRIKE COVERAGE

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

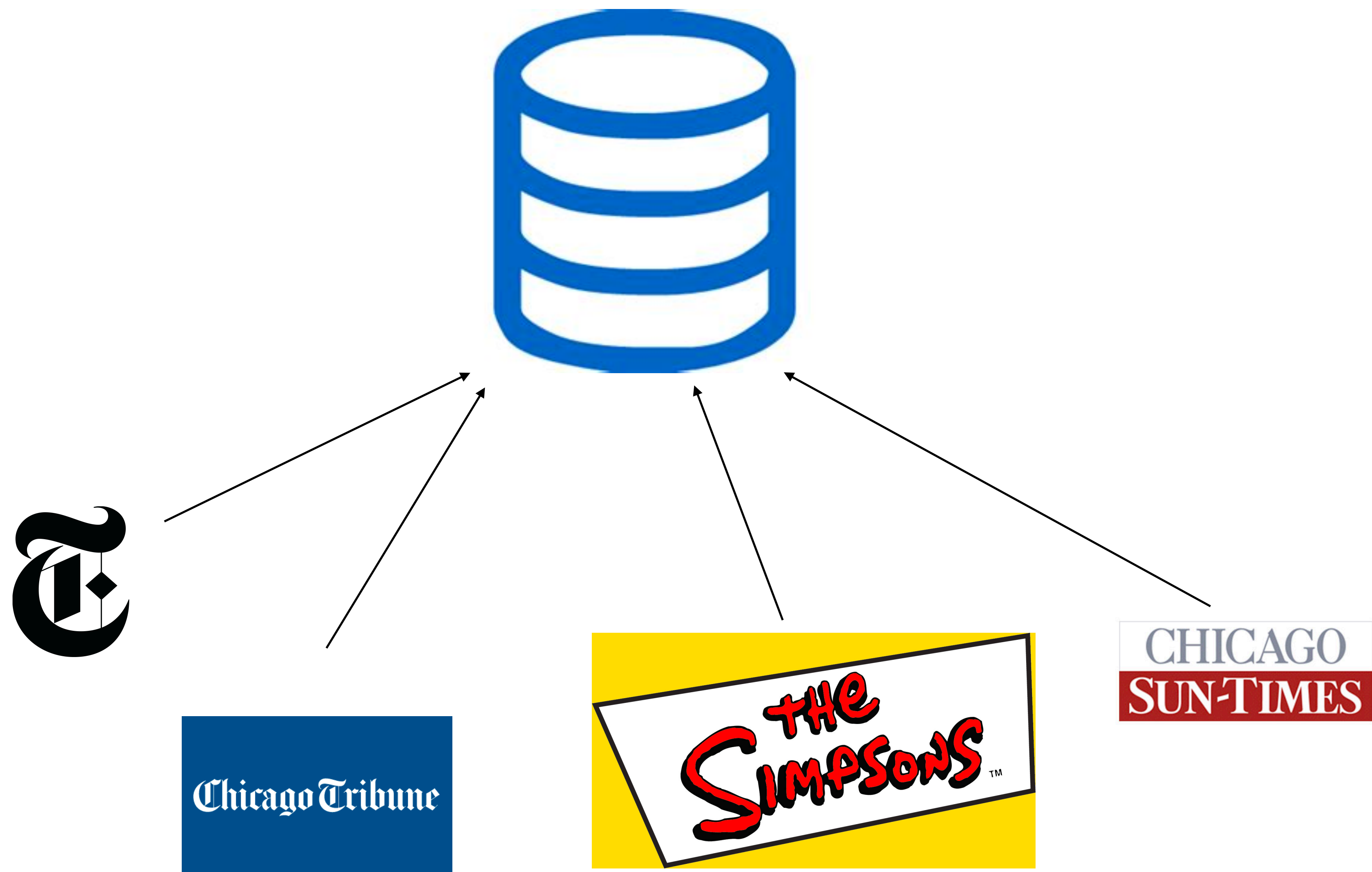
Chicago Park District workers reach contract

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 \(Most of the Time\)](#)

site!

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

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.





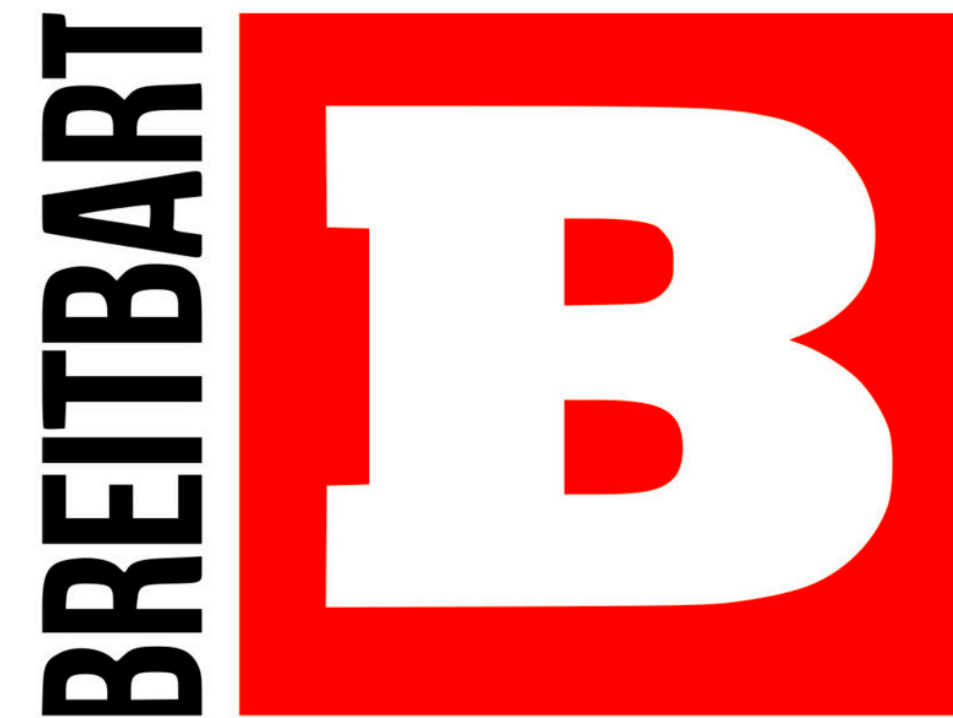
\$ \$ \$

¢ ¢ ¢



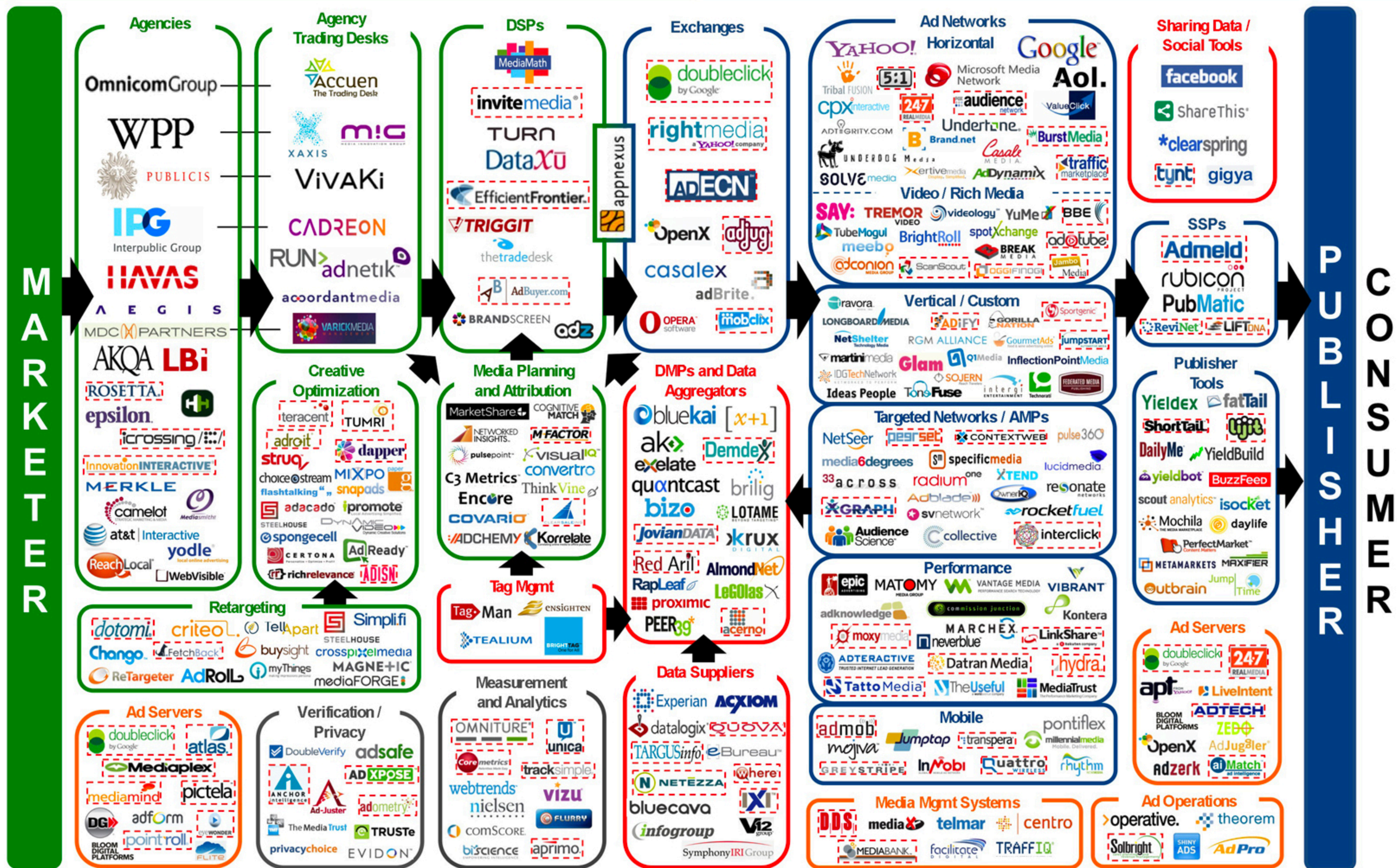


Identify “expensive”
people here



Pay a little to advertise
to them here

DISPLAY LUMAscape



Denotes acquired company

© LUMA Partners LLC 2012

Marketing Technology Landscape

The Martech 5000

Total Solutions 8,000

Advertising & Promotion 922

Content & Experience 1,936

Social & Relationships 1,969

Commerce & Sales 1,314

Data 1,258

Management 601

Access all the data of this landscape & more at martech5000.com

2019
7,040 solutions

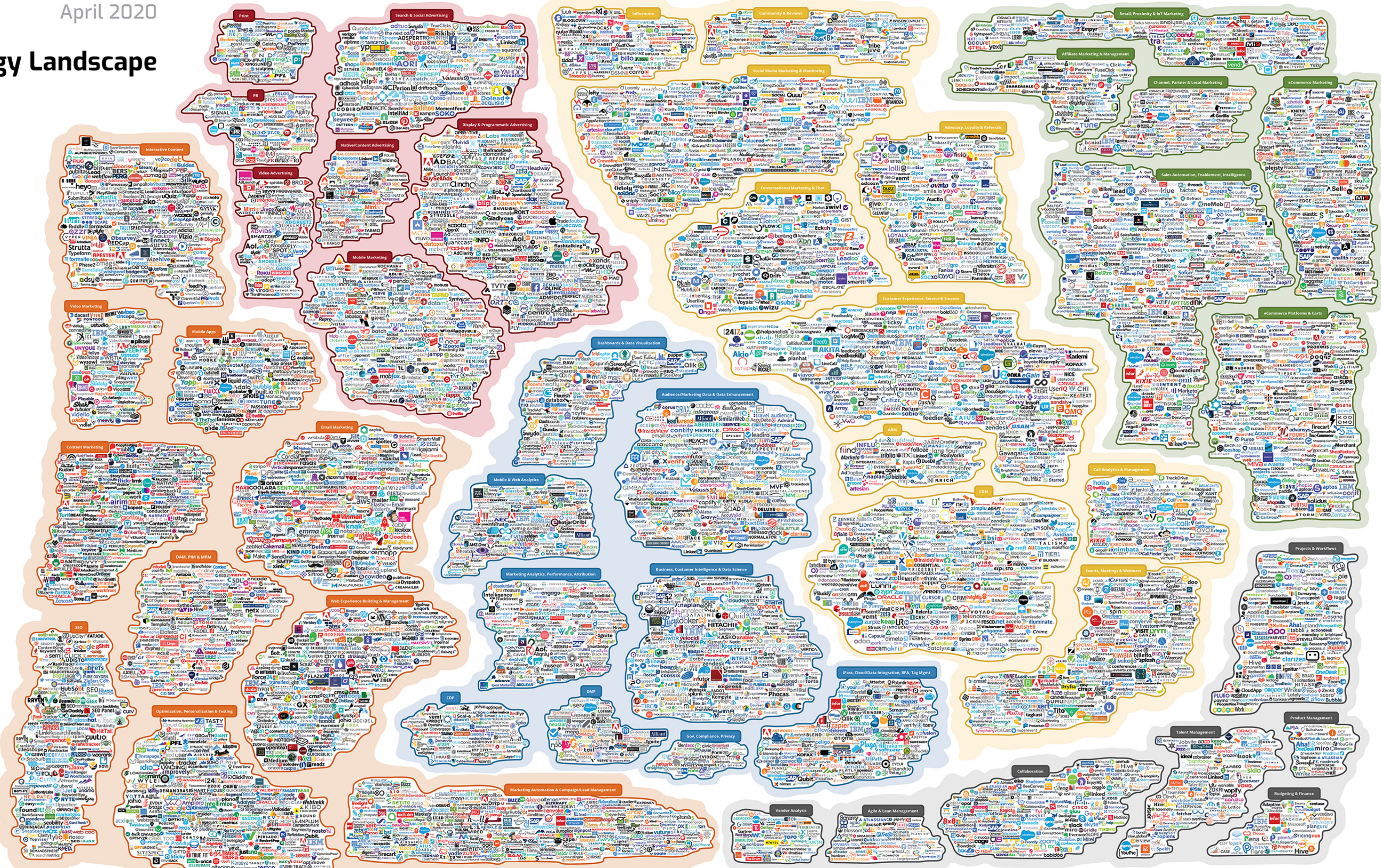
2018
6,829 solutions

2017
5,381 solutions

2016
3,874 solutions

2015
1,876 solutions

2014
947 solutions



Summarizing: Why Does Tracking Matter

- Incompatible with dignity
- Power and control
- Transfers wealth from value-creators to attention-attractors

Overview

- **Why Privacy Matters**
A sloppy manifesto
- **Defining Tracking**
Abstracting the problem
- **Tracking in Practice**
Methods and defenses
- **Privacy Beyond Tracking**
Other issues and concerns



Definitions

- **Website:** eTLD+1 (determined by public suffix list)
e.g., brave.com != mozilla.org
e.g., talk.brave.com == search.brave.com
e.g., ted.github.io != betty.github.io
- **Origin:** The full DNS host name serving a site
- **First-party:** Site of the top level document
- **Third-party:** any other site

Definitions (more)

- **DOM Storage:** Explicit storage APIs
e.g., cookies, localStorage, IndexedDB
- **Network State:** All other storage
e.g., caches (v8, DNS, HTTP)
e.g., Header instructions (HSTS, ALT-SRV, etc)
- **Online Tracking**
Its trickier...

A Rough Definition of Tracking

- **Linking activities...**
e.g., being “followed”
- **across boundaries...**
e.g., temporal, geographic,
conceptual
- **In a way not expected or desired.**
e.g., ignorance or non-consent

Tracking in Context

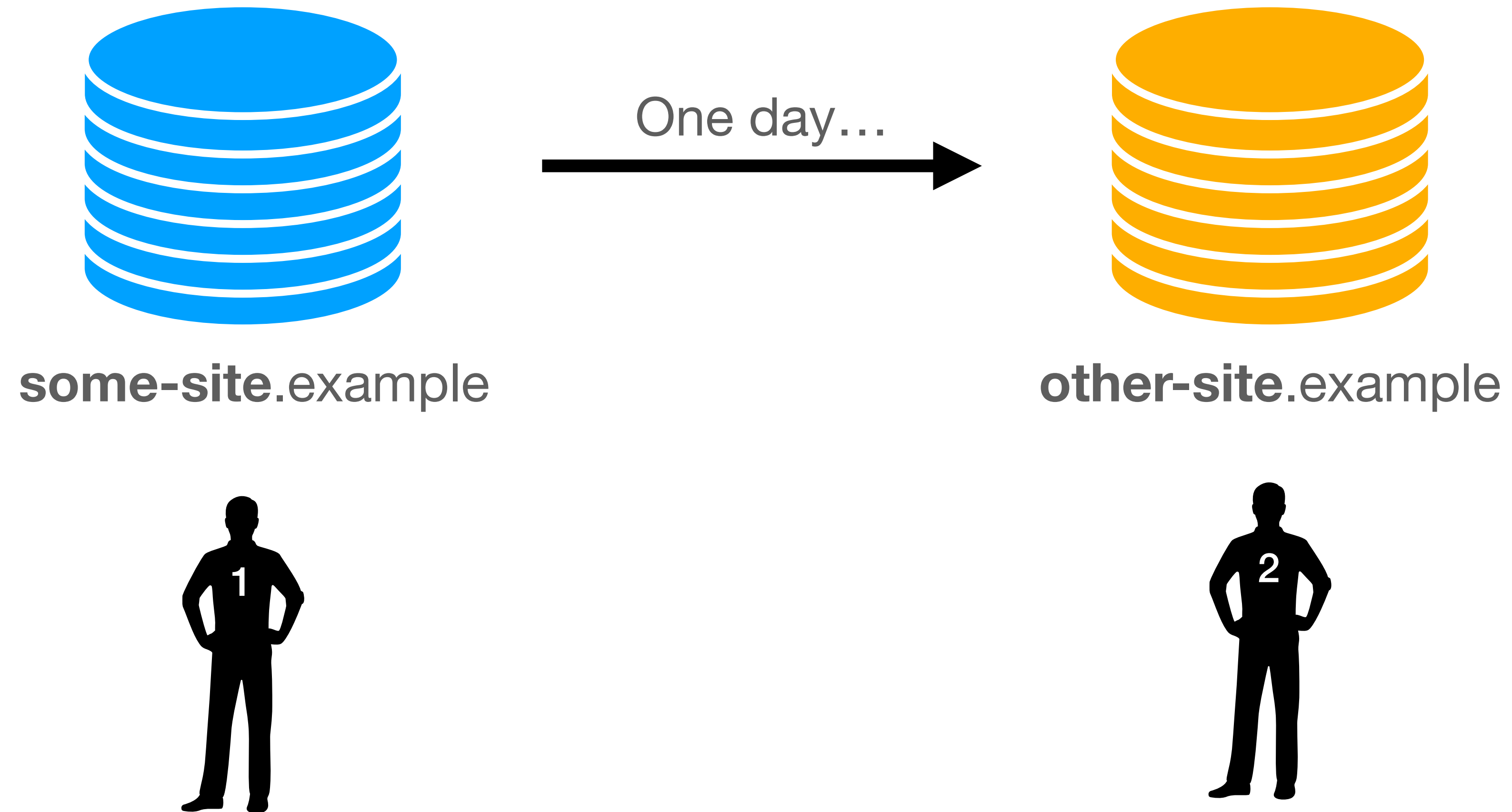


A Rough Definition of Tracking

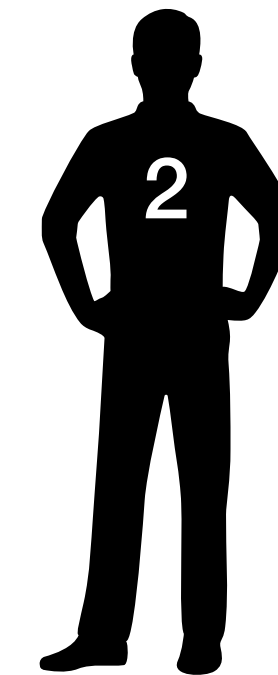
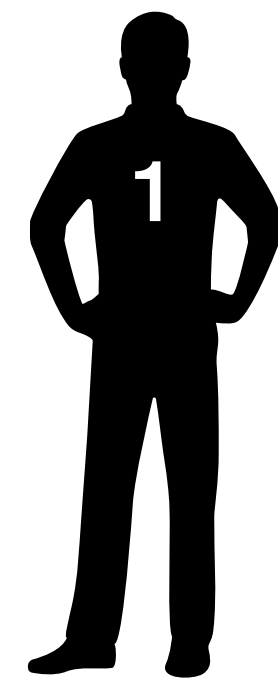
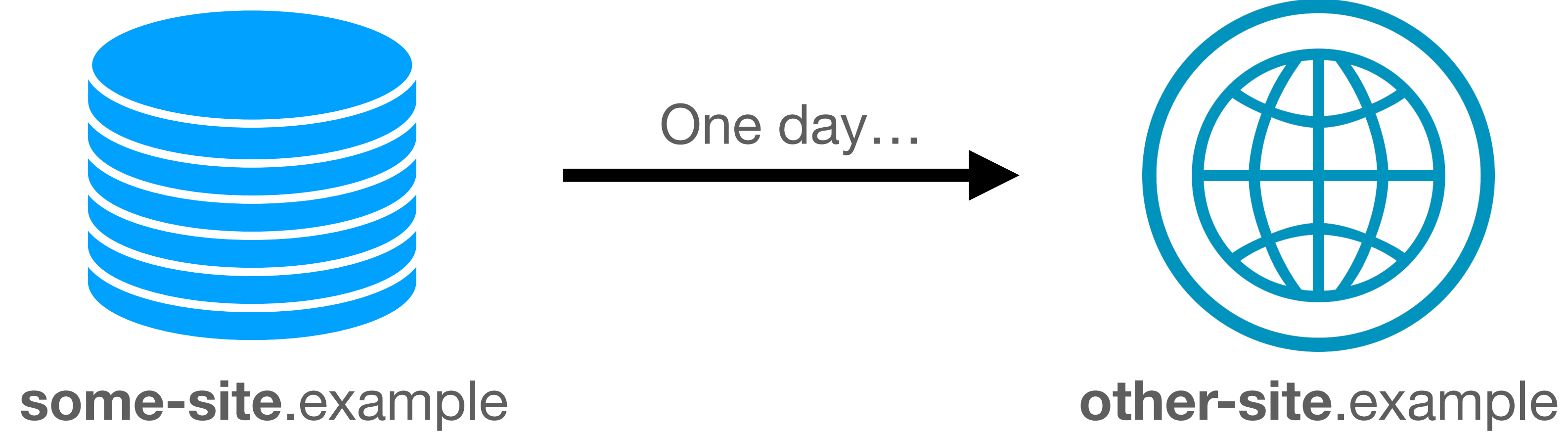
- **Linking activities...**
e.g., being “followed”
- **across boundaries...**
e.g., temporal, geographic,
conceptual
- **In a way not expected or desired.**
e.g., ignorance or non-consent



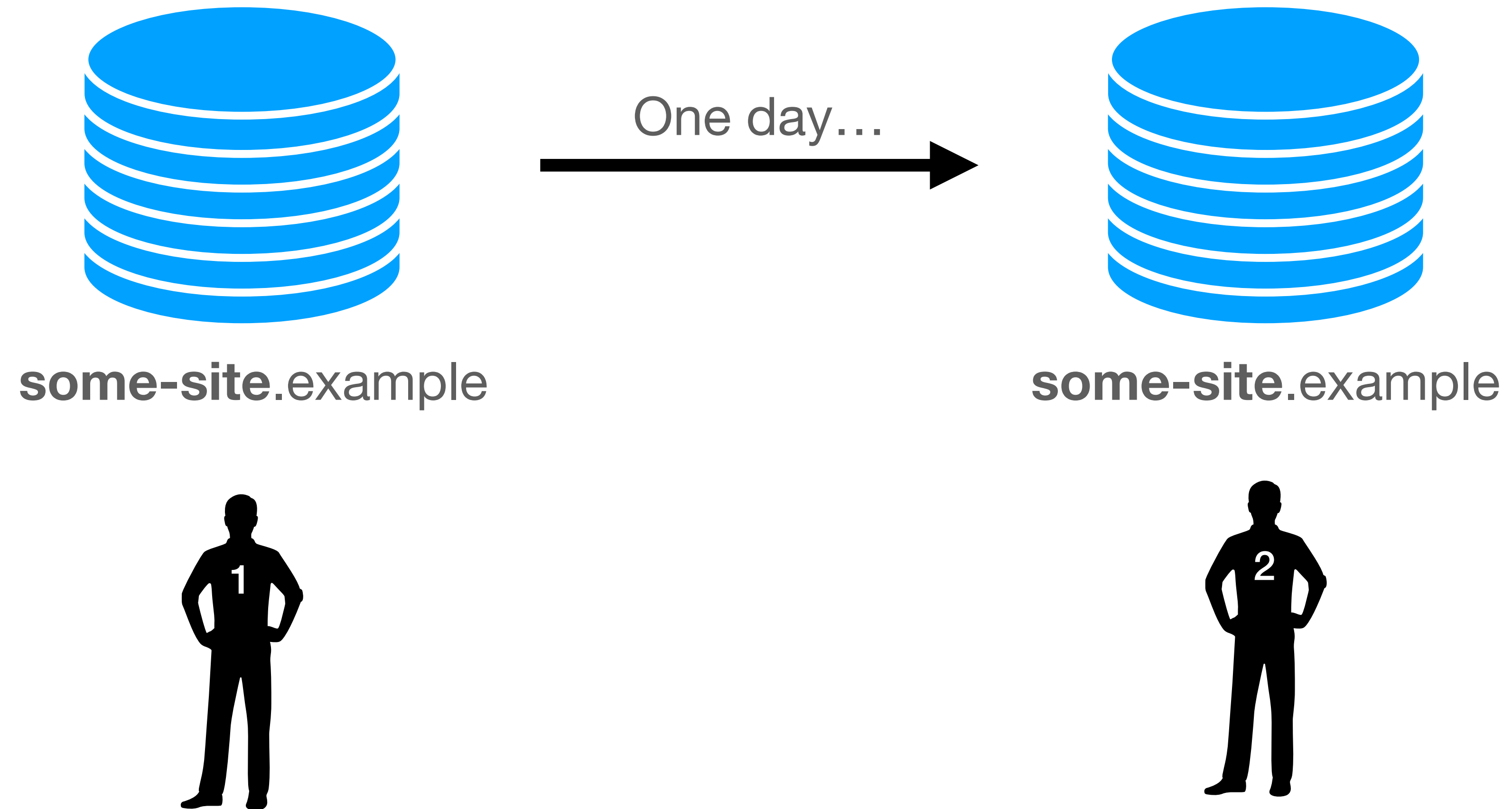
Question One



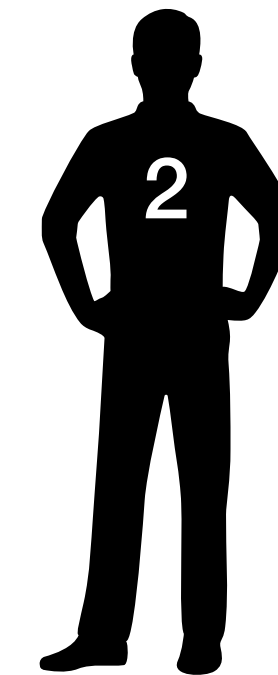
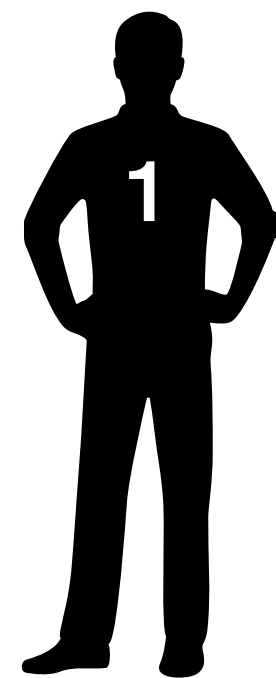
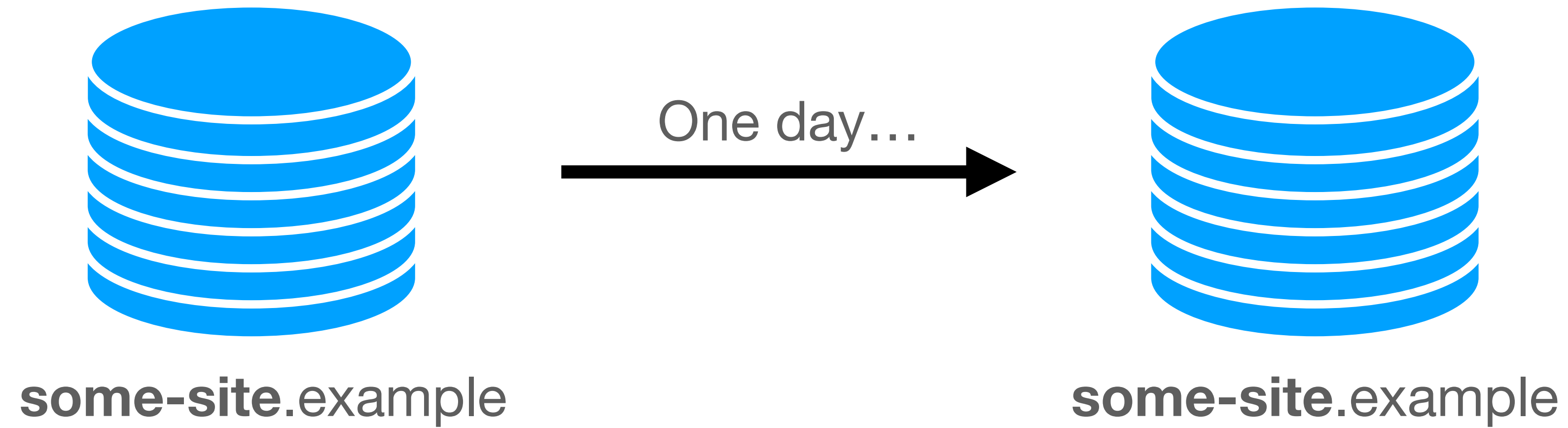
Question One



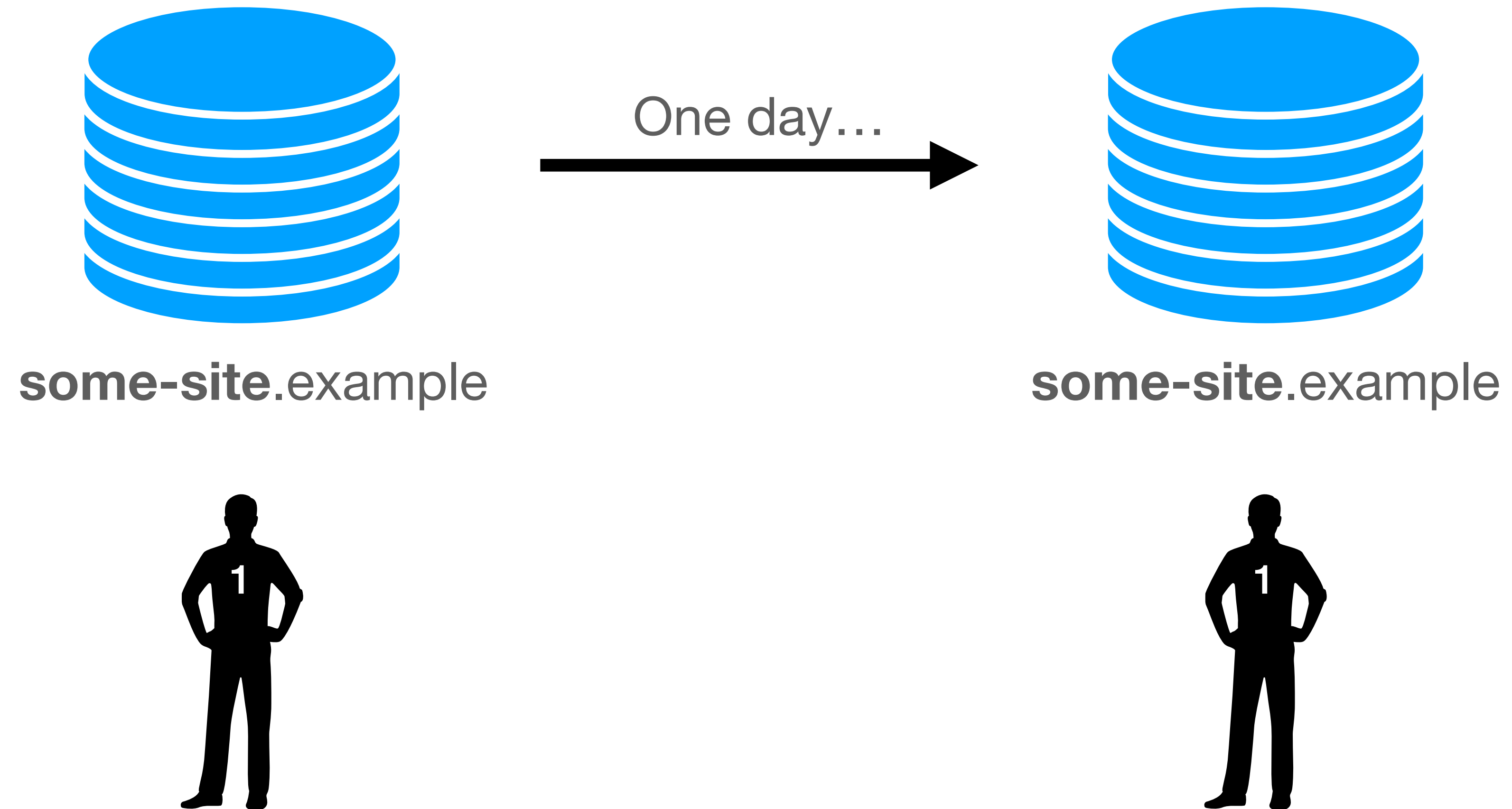
Question Two



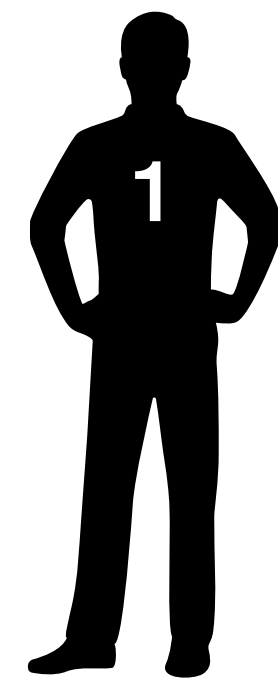
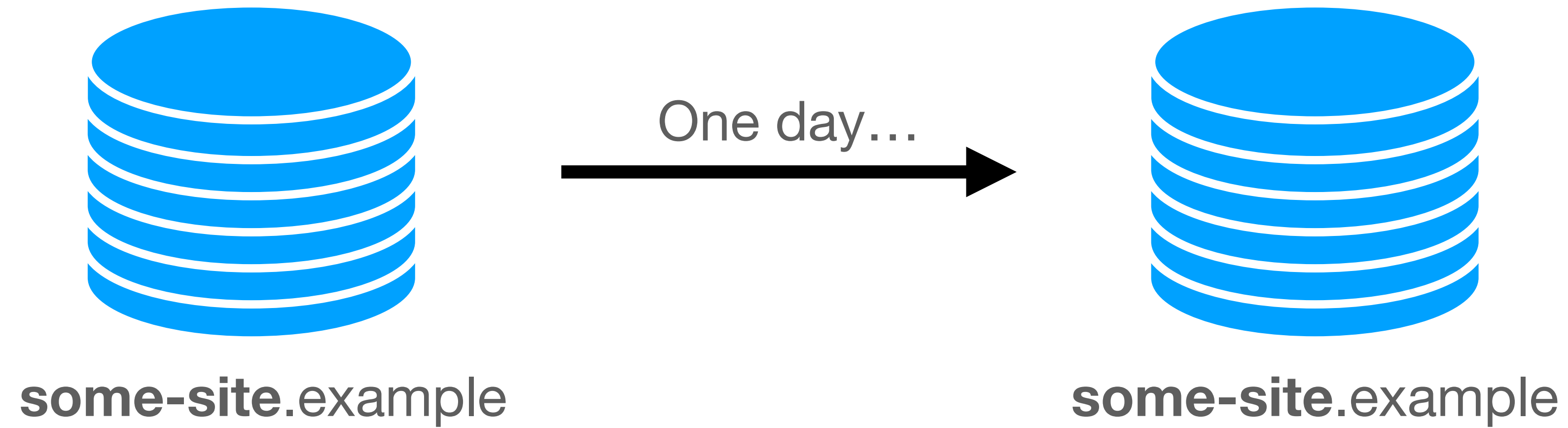
Question Two



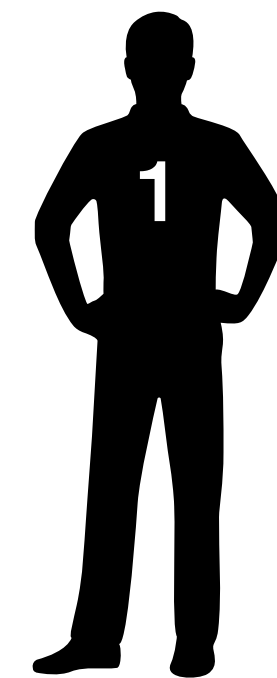
Question Three



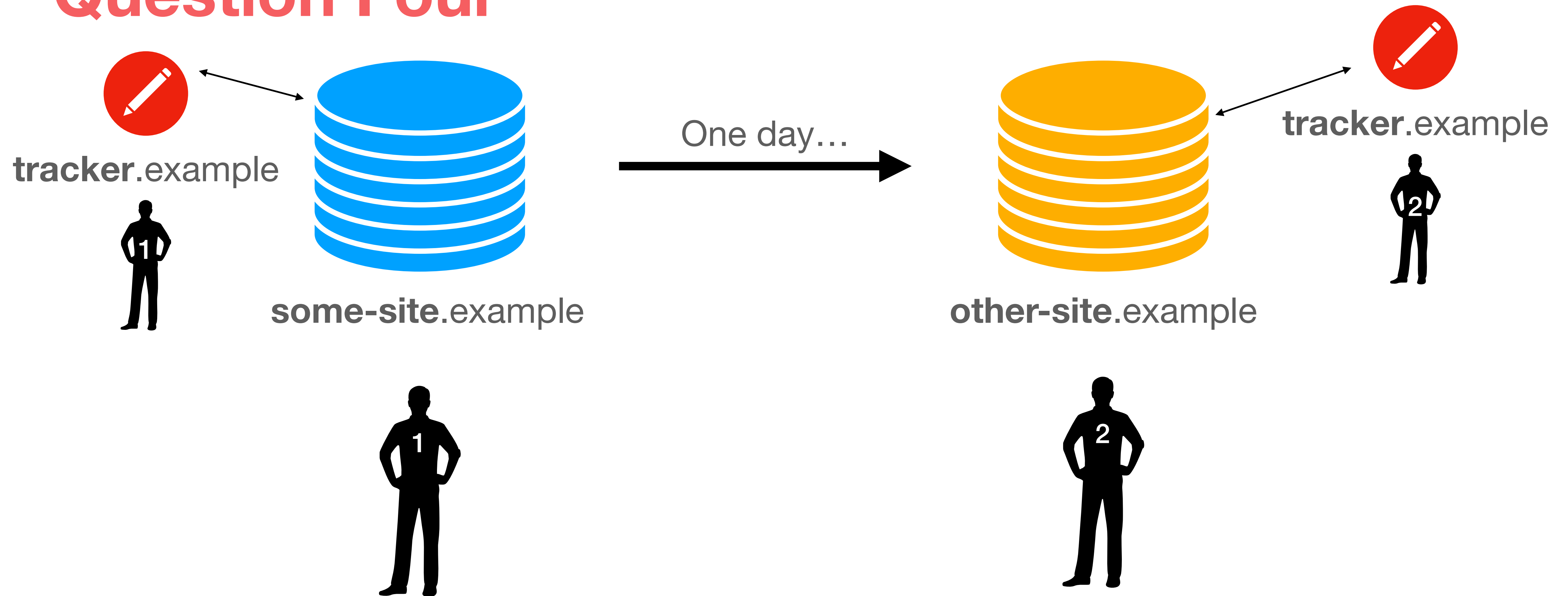
Question Three



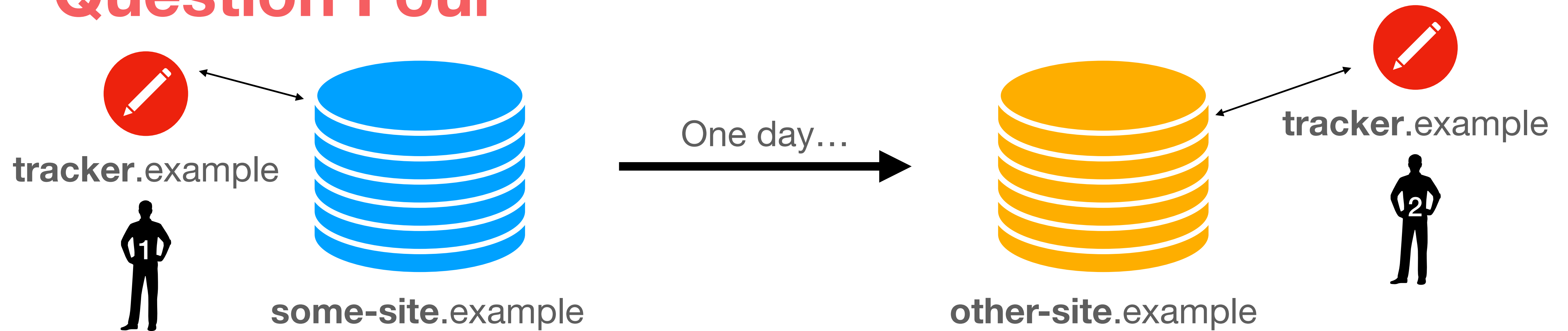
Linking
(first-party)



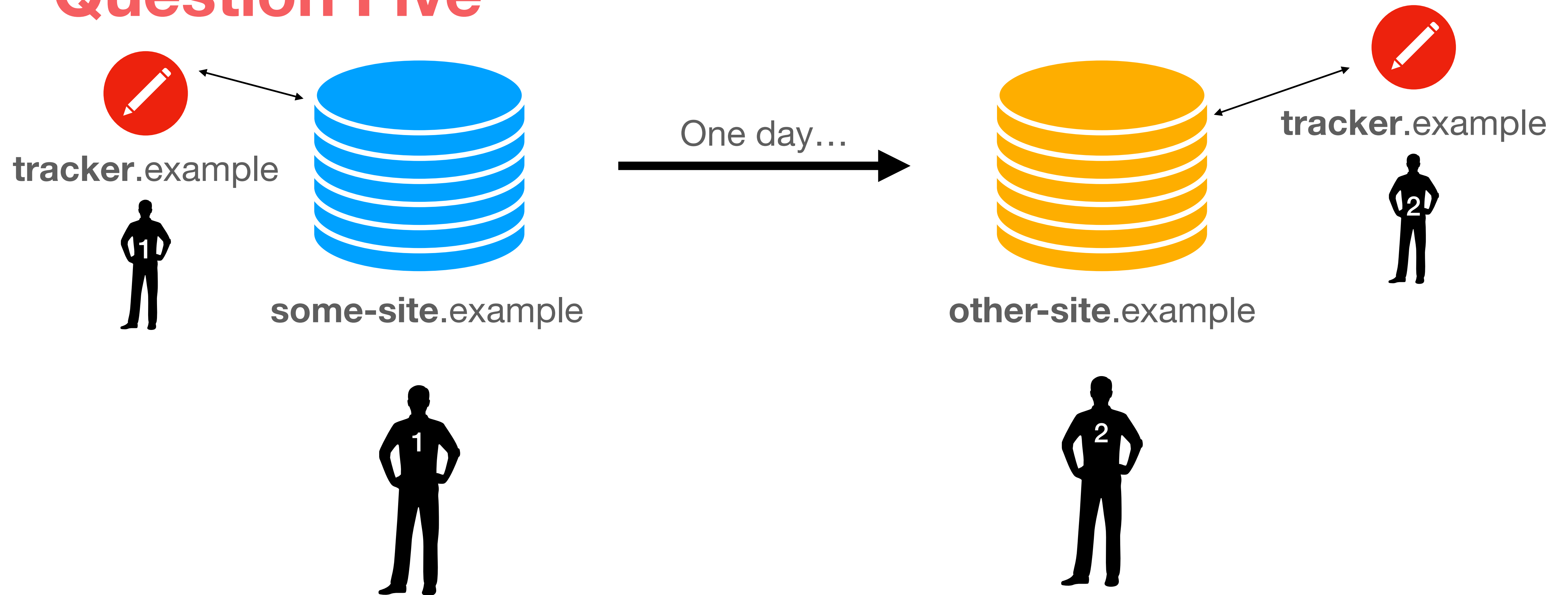
Question Four



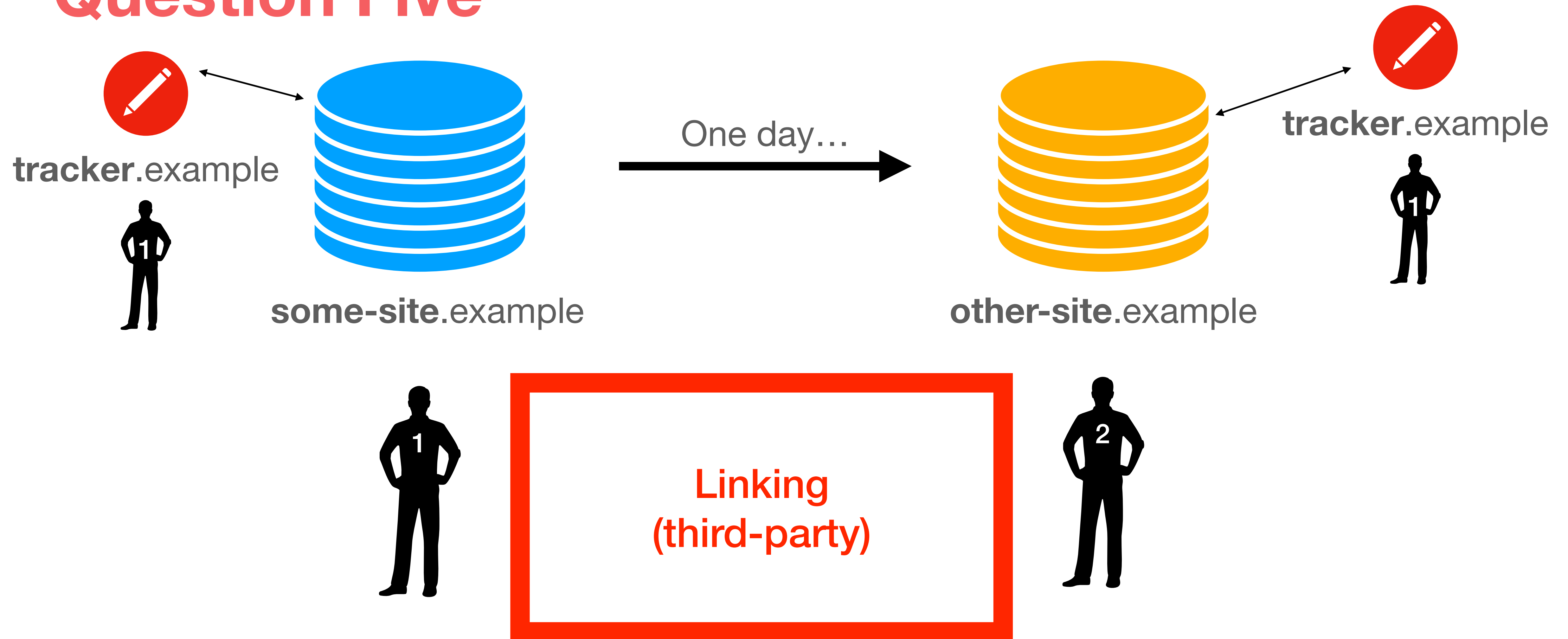
Question Four



Question Five



Question Five



Tracking: Linking...

- **Tying behaviors to same identity**
Could be pseudonymous, or a “real world” identity
- **Probabilistic or deterministic**
For some definition of “probable enough”

A Rough Definition of Tracking

- **Linking activities...**
e.g., being “followed”
- **across boundaries...**
e.g., temporal, geographic,
conceptual
- **In a way not expected or desired.**
e.g., ignorance or non-consent



Tracking: ...across boundaries...

- **Organizational boundaries**
e.g., eTLD+1, origin, “first-party set”
- **Temporal boundaries**
e.g., tying something done last year to something done today
- **Profile boundaries**
e.g., private browsing, different browsers, accounts

A Rough Definition of Tracking

- **Linking activities...**
e.g., being “followed”
- **across boundaries...**
e.g., temporal, geographic,
conceptual
- **In a way not expected or desired.**
e.g., ignorance or non-consent



Tracking: ...expectations

- **Expectations differ across platforms**
Facebook inapp browser vs Tor Browser Bundle
- **Expectations differ across people's expertise**
e.g., my dad vs Dworkin
- **Expectations differ across backgrounds**
e.g., outlook.com vs microsoft.com vs github.com
- **Consent is (sometimes) fuzzy**
Terms of service <— — — — — — — —> Storage Access API

A Rough Definition of Tracking

- **Linking activities...**
e.g., being “followed”
- **across boundaries...**
e.g., temporal, geographic,
conceptual
- **In a way not expected or desired.**
e.g., ignorance or non-consent

Overview

- **Why Privacy Matters**
A sloppy manifesto
- **Defining Tracking**
Abstracting the problem
- **Tracking in Practice**
Methods and defenses
- **Privacy Beyond Tracking**
Other issues and concerns



Tracking Techniques

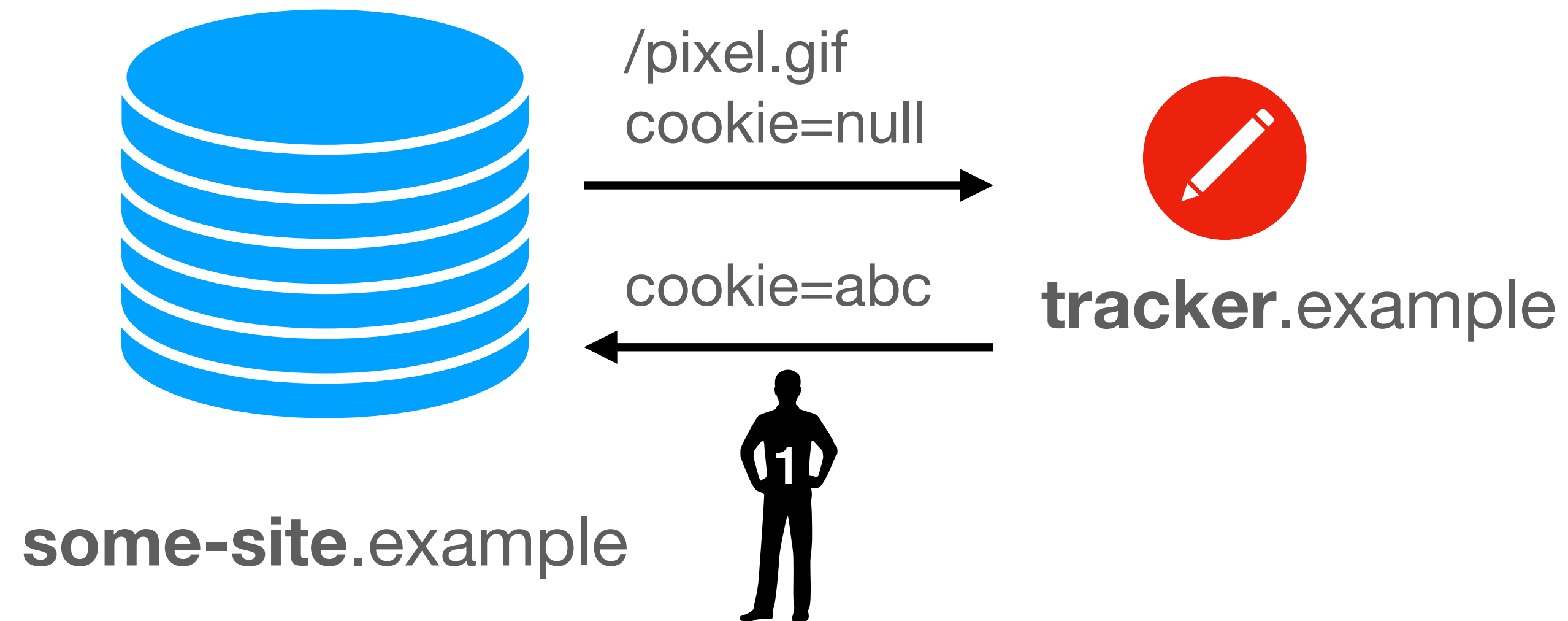
- **Third-party DOM storage**
- **Network state**
- **Bounce tracking**
- **Browser fingerprinting**
- **IP address**
- **Personal identifiers**

Tracking Techniques

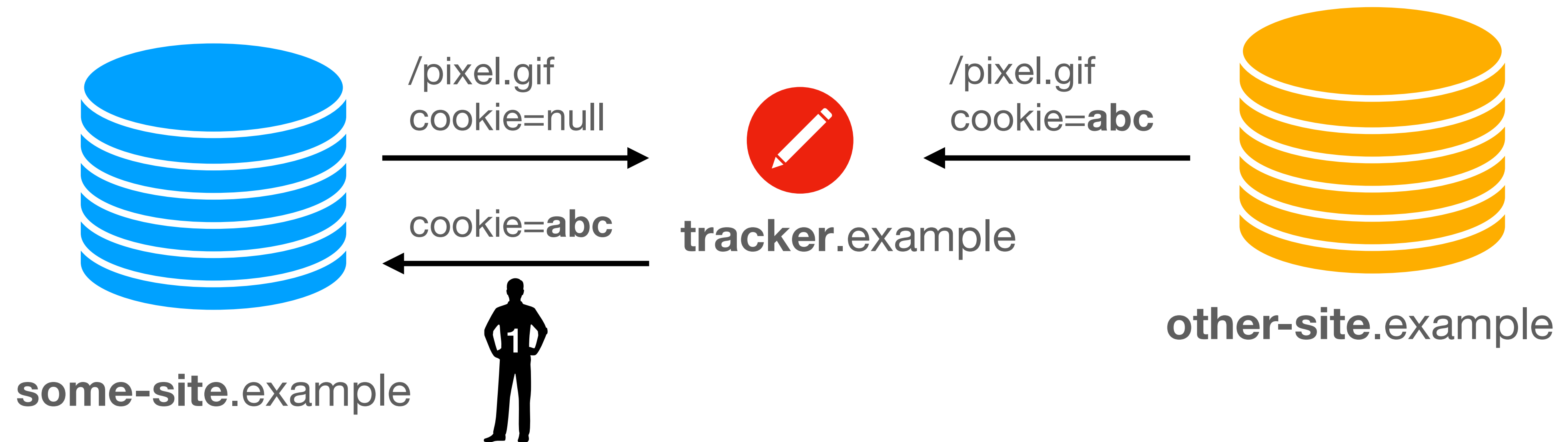
- Third-party DOM storage
- Network state
- Bounce tracking
- Browser fingerprinting
- IP address
- Personal identifiers



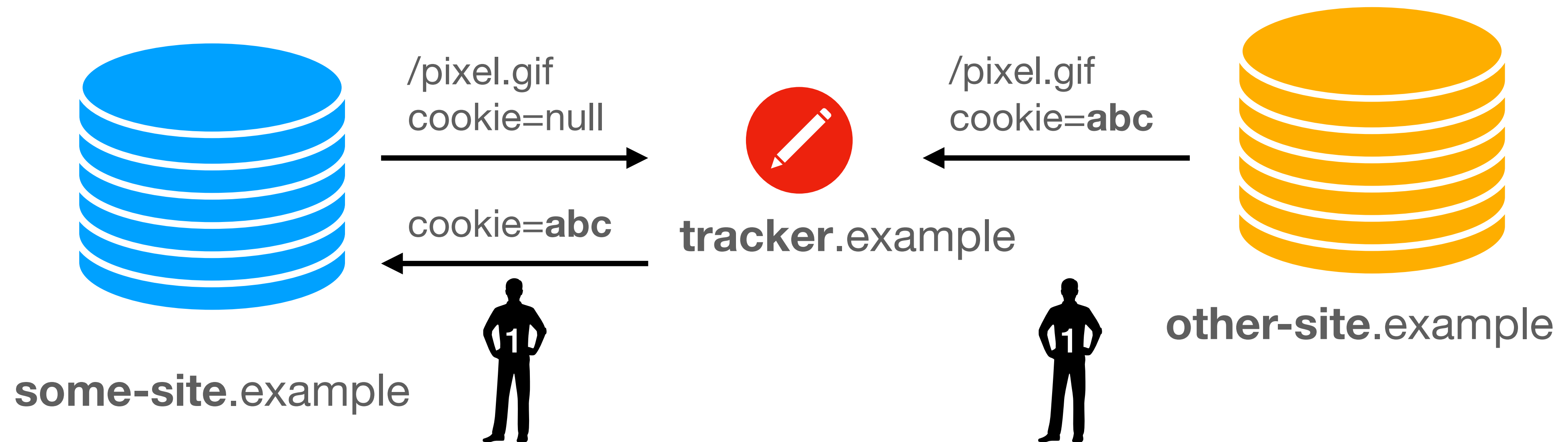
Third-party DOM storage



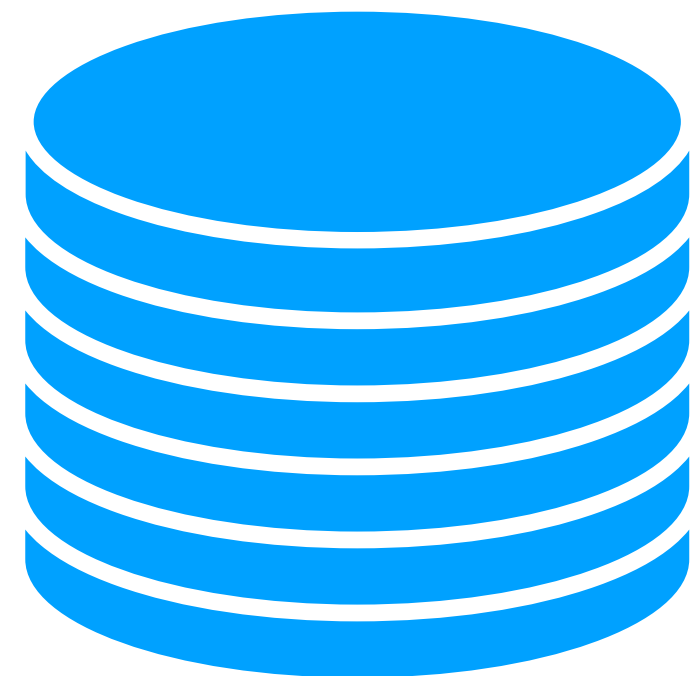
Third-party DOM storage: cookies



Third-party DOM storage: cookies



Third-party DOM storage: iframe



some-site.example

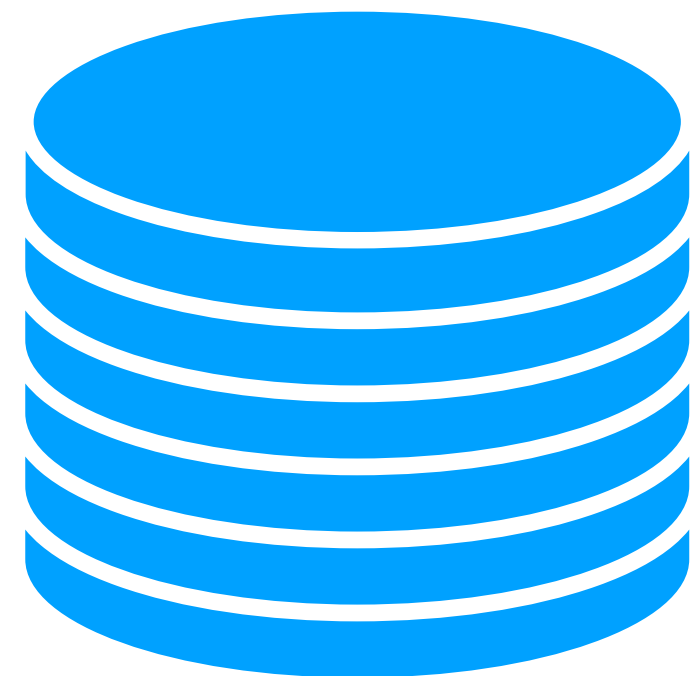
```
<iframe src=//tracker.example>
const LS = localStorage

if (LS['id']) {
  // I re-identified a person
} else {
  // new person, assigning ID
  LS['id'] = Math.random()
}

fetch(`/record?id=${LS['id']}`)

</iframe>
```

Third-party DOM storage: iframe



some-site.example

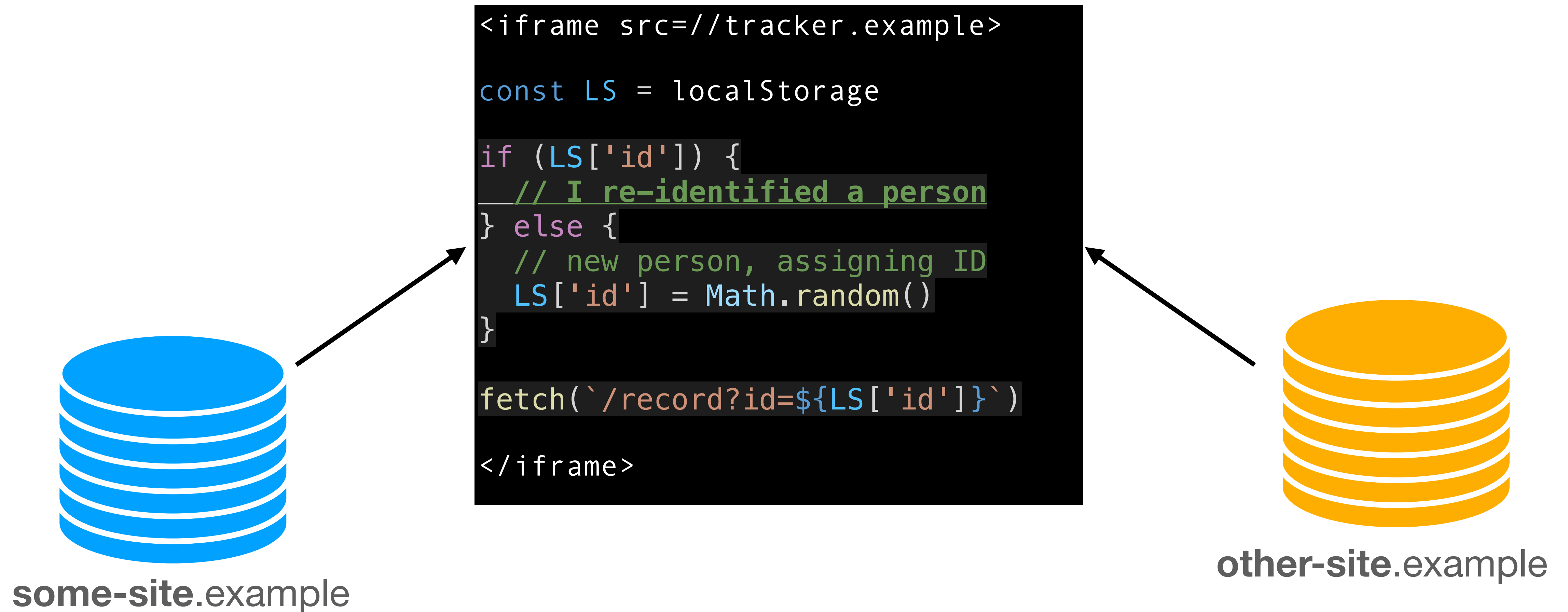
```
<iframe src=//tracker.example>
const LS = localStorage

if (LS['id']) {
  // I re-identified a person
} else {
  // new person, assigning ID
  LS['id'] = Math.random()
}

fetch(`/record?id=${LS['id']}`)

</iframe>
```

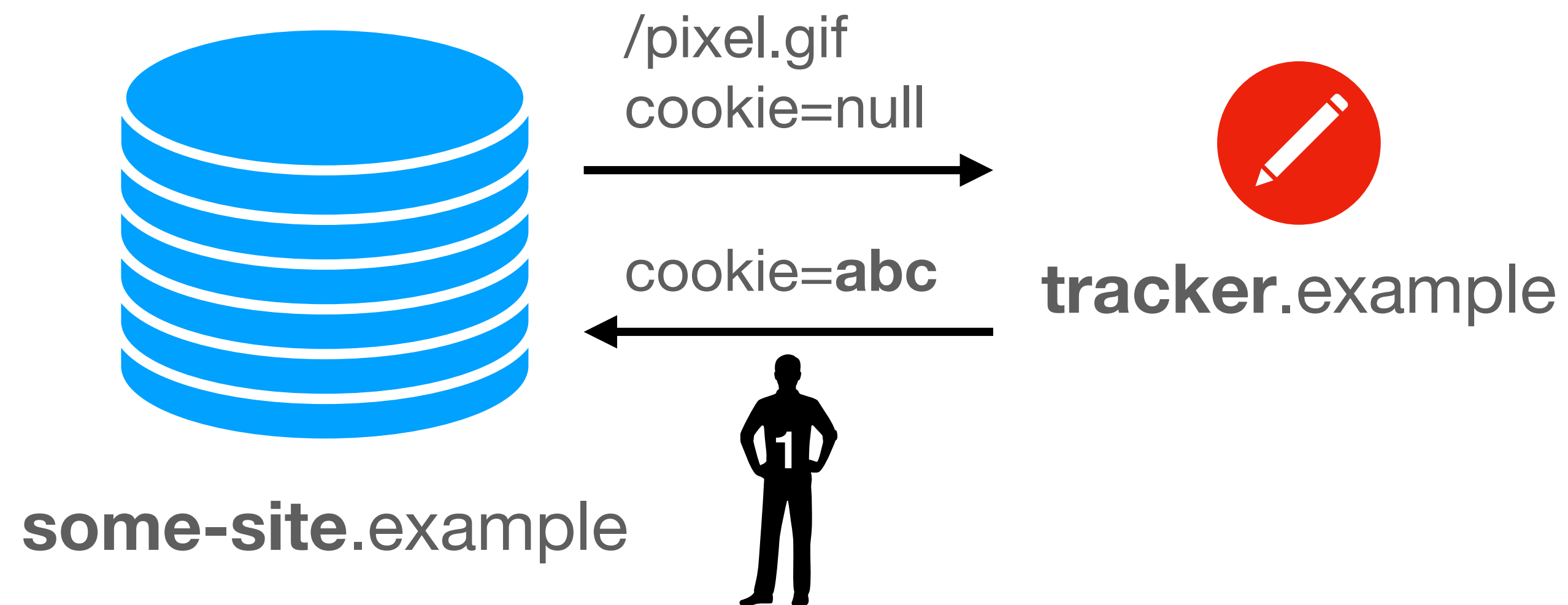

Third-party DOM storage: iframe



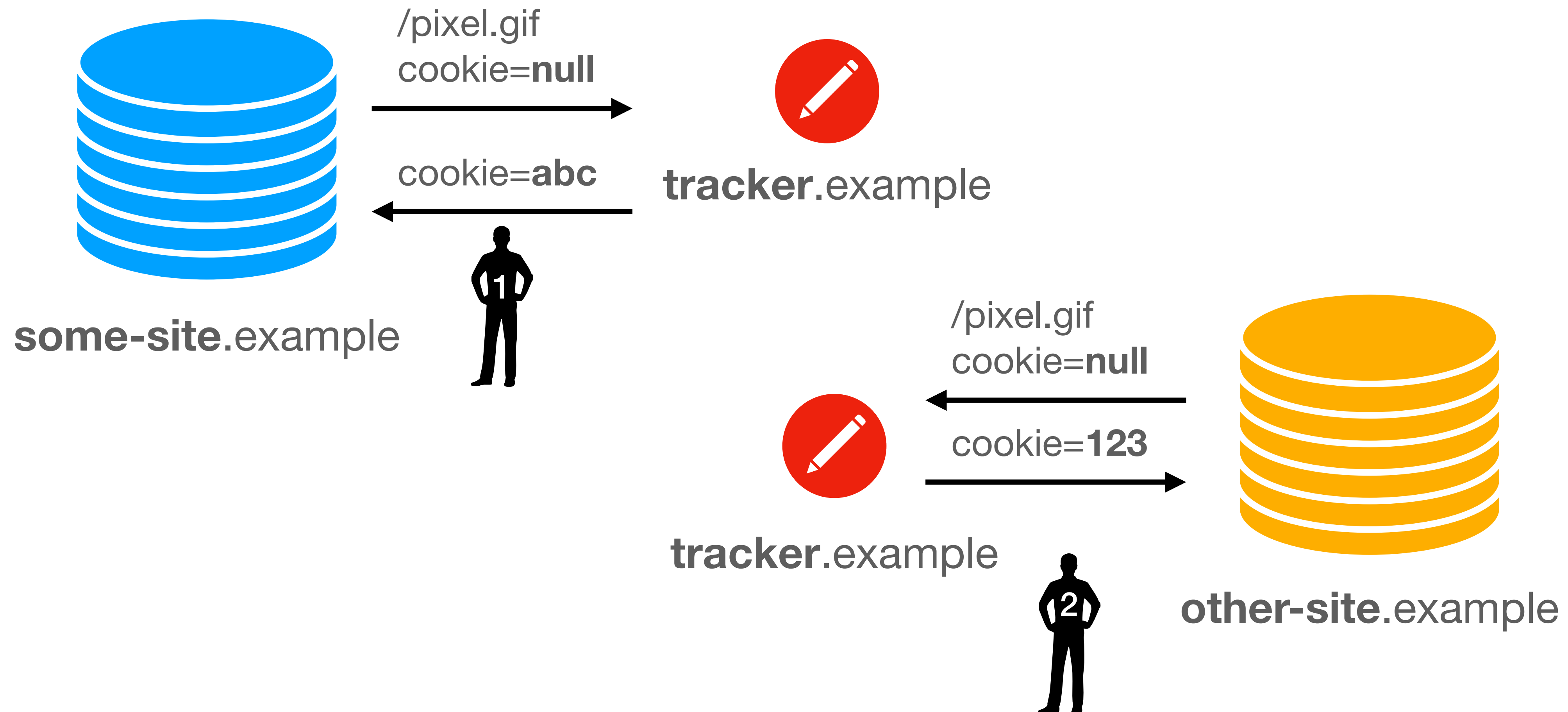
Third-party DOM storage: partitioning

- Third-party storage is not shared across sites
- Sometimes called “dual-keying”
- Previous:
`storage_data = browser_storage[<requested eTLD+1>]`
- Partitioning:
`storage_data = browser_storage[<first-party eTLD+1>][<requested eTLD+1>]`









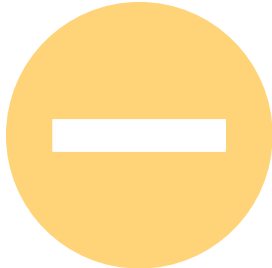
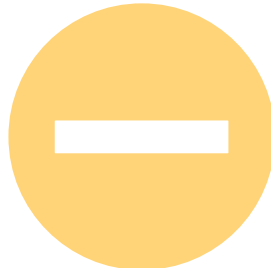
Third-party DOM storage: partitioning



Third-party DOM storage: partitioning



Third-party DOM storage: Defenses

	Chrome	Safari	Edge	Firefox	Brave
Block third-party cookies					
Partition storage					
Ephemeral partitions					
List based defenses					

Tracking Techniques

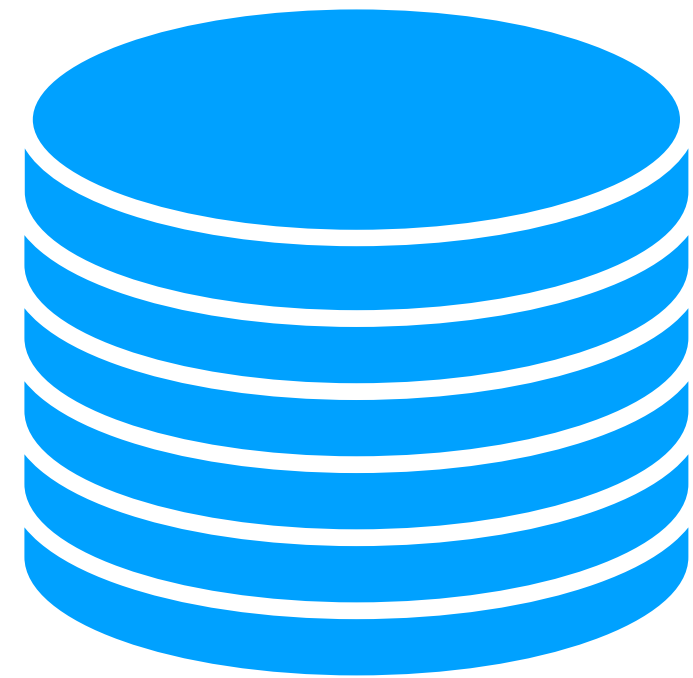
- Third-party DOM storage
- Network state
- Bounce tracking
- Browser fingerprinting
- IP address
- Personal identifiers



Network State Example: HTTP Cache

- **Browsers cache things for speed**
Images, JavaScript, etc.
- **Caches are generally unpartitioned**
- **Anything unpartitioned can be a linking key**

HTTP Cache Tracking



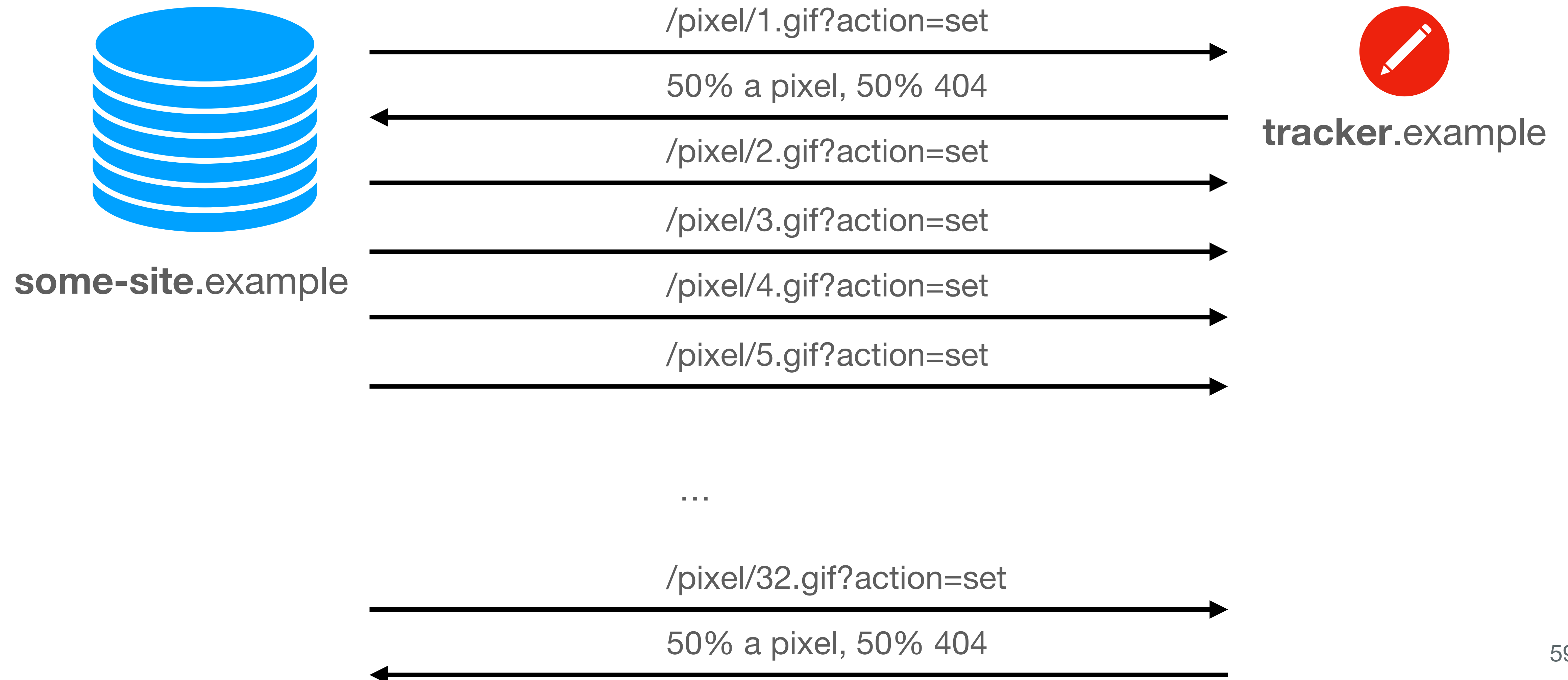
some-site.example



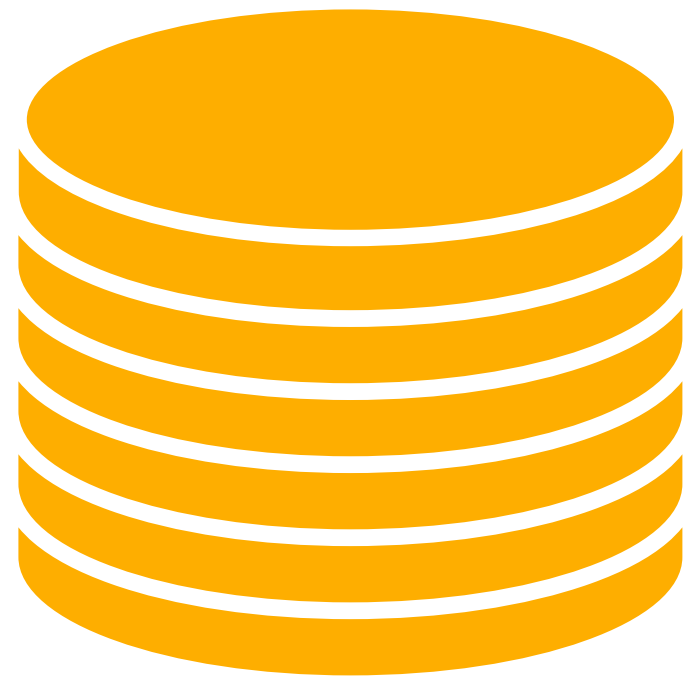
tracker.example

- `/pixel/#.gif?action={set, read}`
- `action=set`: 50% return pixel
: 50% 404
- `action=read`: 100% 404

HTTP Cache Tracking



HTTP Cache Tracking



other-site.example

<https://tracker.example/script.js>



tracker.example

```
const identifier = []
for (let i = 0; i < 32; i += 1) {
  try {
    const url = `/pixel/${i}.gif?action=read`
    await fetch(url)
    // We hit the cache
    identifier[i] = 1
  } catch (_) {
    // We missed the cache
    identifier[i] = 0
  }
}
// identifier is now a unique 32 bits
```

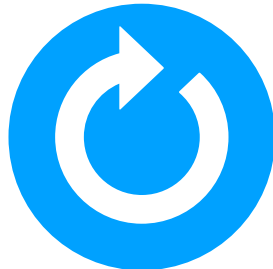
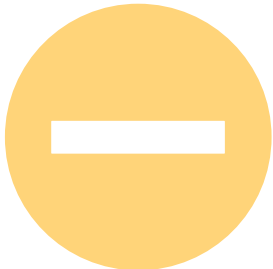

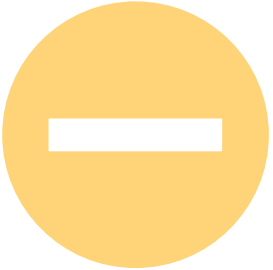
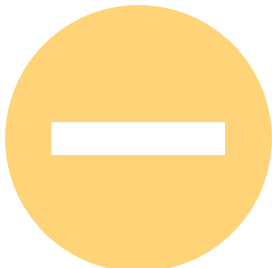
HTTP Strict Transport Security (HSTS)

- **Website Says “only HTTPS, forever”**
e.g. persistent storage
- **Automatic Upgrade**
`http://example.org -> https://example.org`
- **How to leverage?**

HSTS Tracking

- **example.org**
- **a.example.org**
- **b.example.org**
- **a.a.example.org**
- **b.a.example.org**

Network state: Defenses

	Chrome	Safari	Edge	Firefox	Brave
Partition network state					
List based defenses					

Tracking Techniques

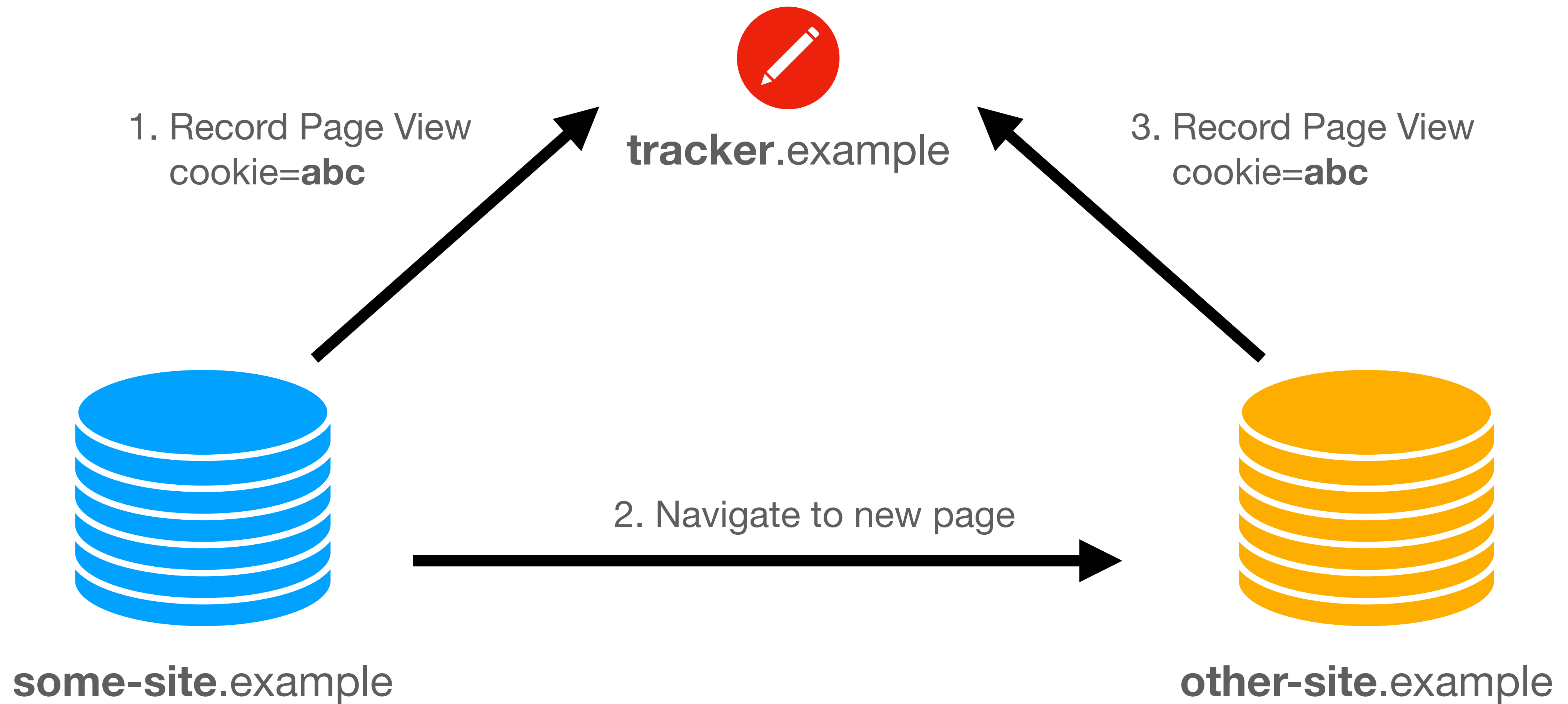
- Third-party DOM storage
- Network state
- Bounce tracking
- Browser fingerprinting
- IP address
- Personal identifiers



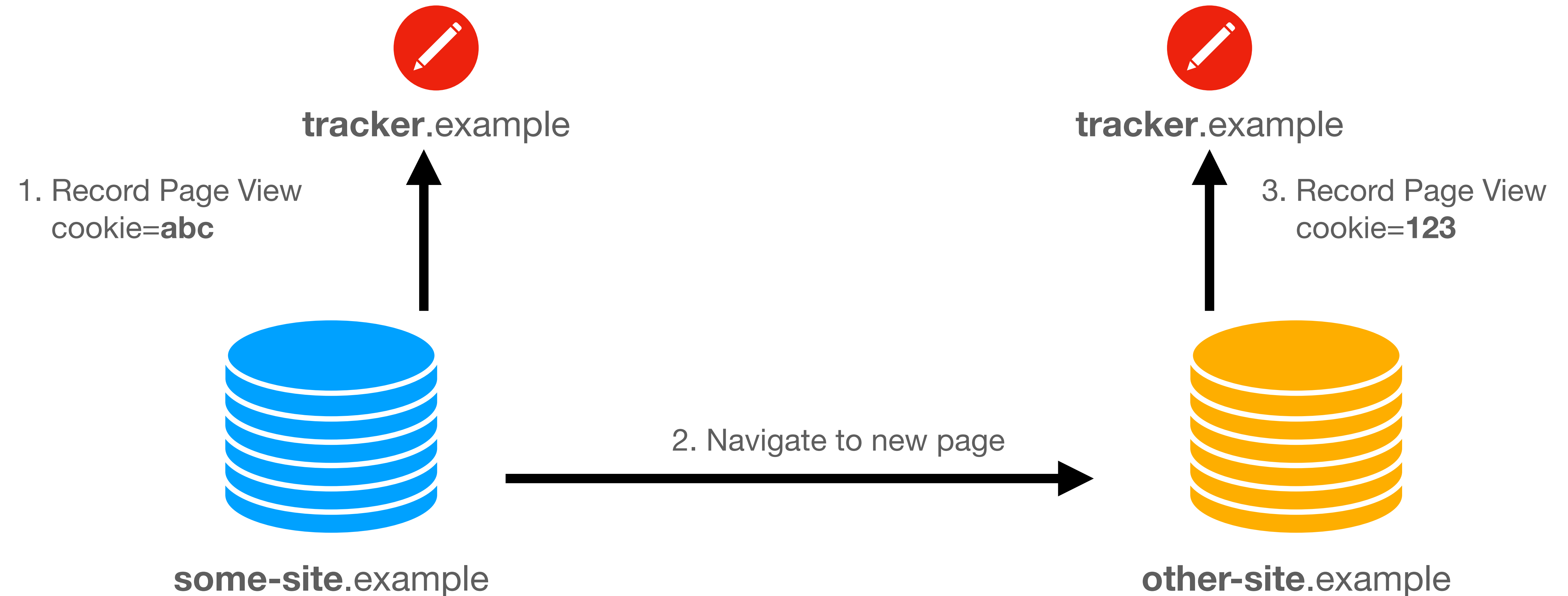
Bounce Tracking

- **Response to partitioning**
- **Third parties use first-parties to track**
- **Growing in importance as partitioning is more common**

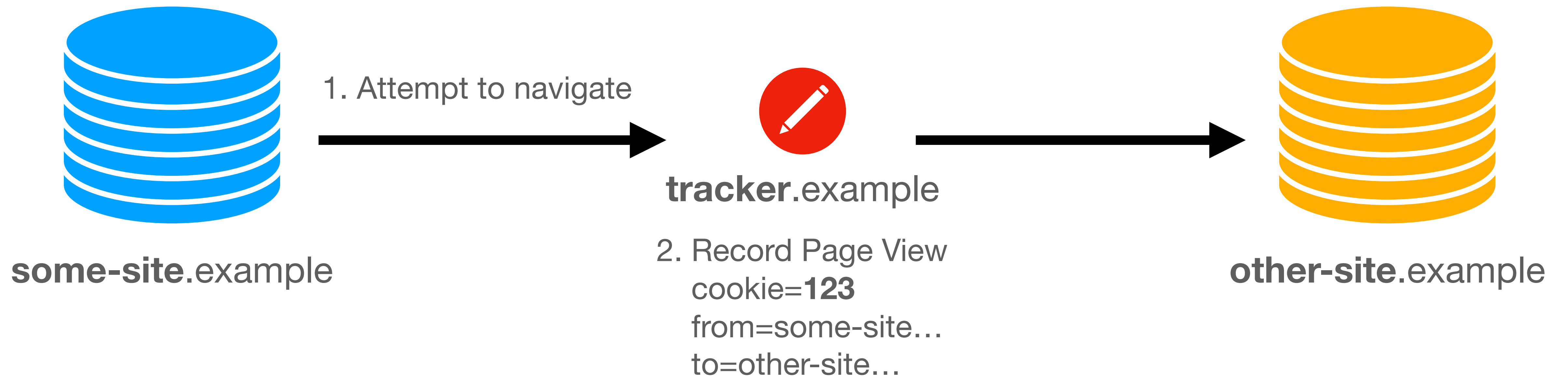
Pre-partitioning



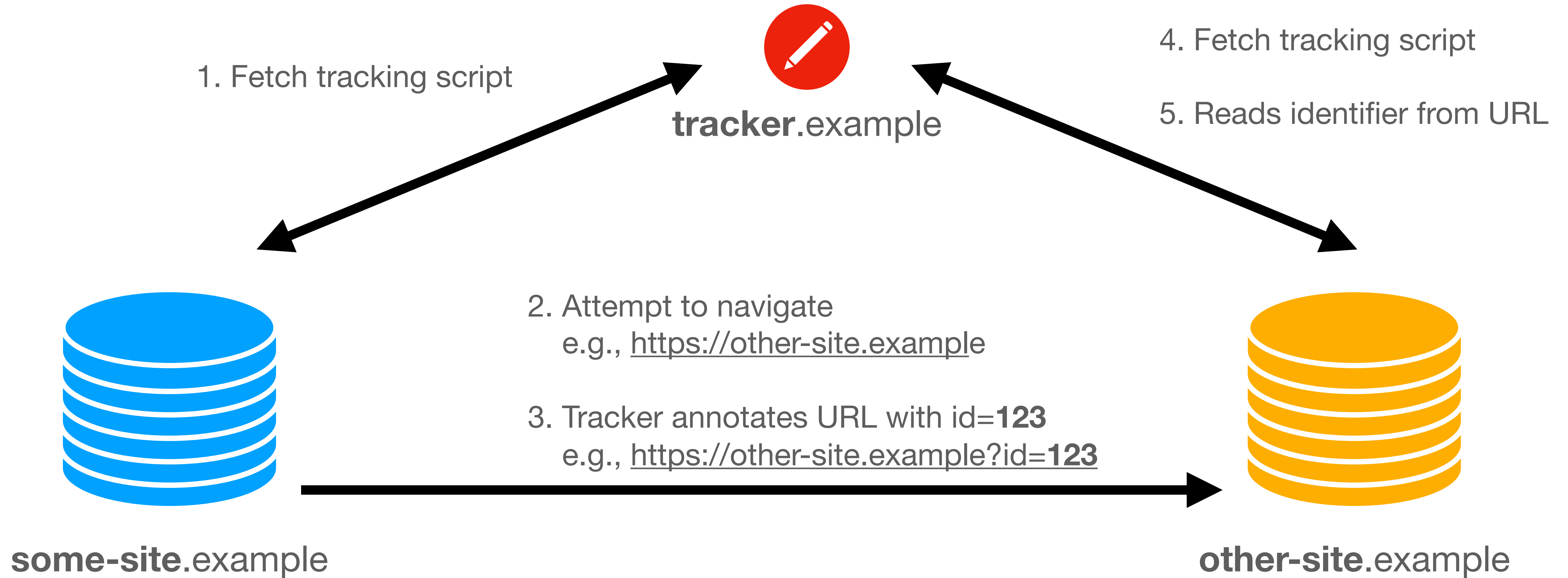
Storage partitioning





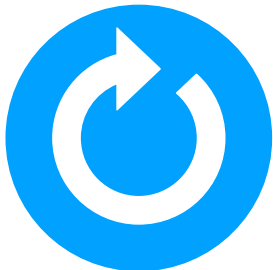
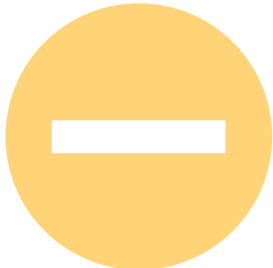
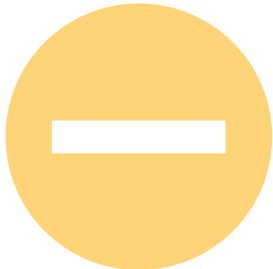
Bounce tracking



Navigation tracking



Bounce and Navigation Tracking: Defenses

	Chrome	Safari	Edge	Firefox	Brave
Limit storage		heuristic 		List 	
“Debounce”					List 
Warn user					List 

Tracking Techniques

- Third-party DOM storage
- Network state
- Bounce tracking
- Browser fingerprinting
- IP address
- Personal identifiers



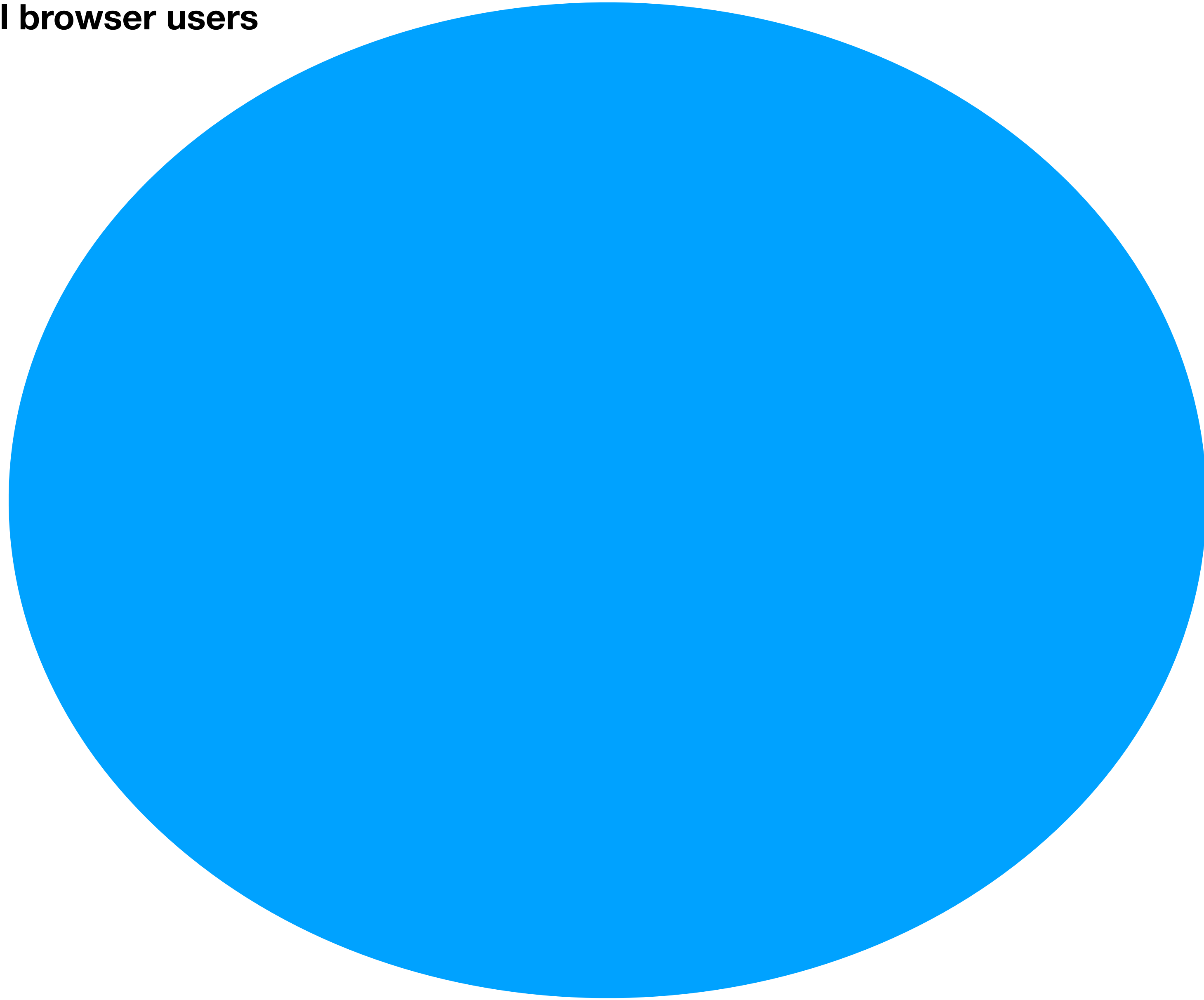
Fingerprinting, contrasted

- **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
 - “Stateful”
- **Fingerprinting / passive tracking**
 - Website finds things different about each visitor
 - Tracker derives the identifier from minor browser differences
 - “Stateless”

Fingerprinting, how?

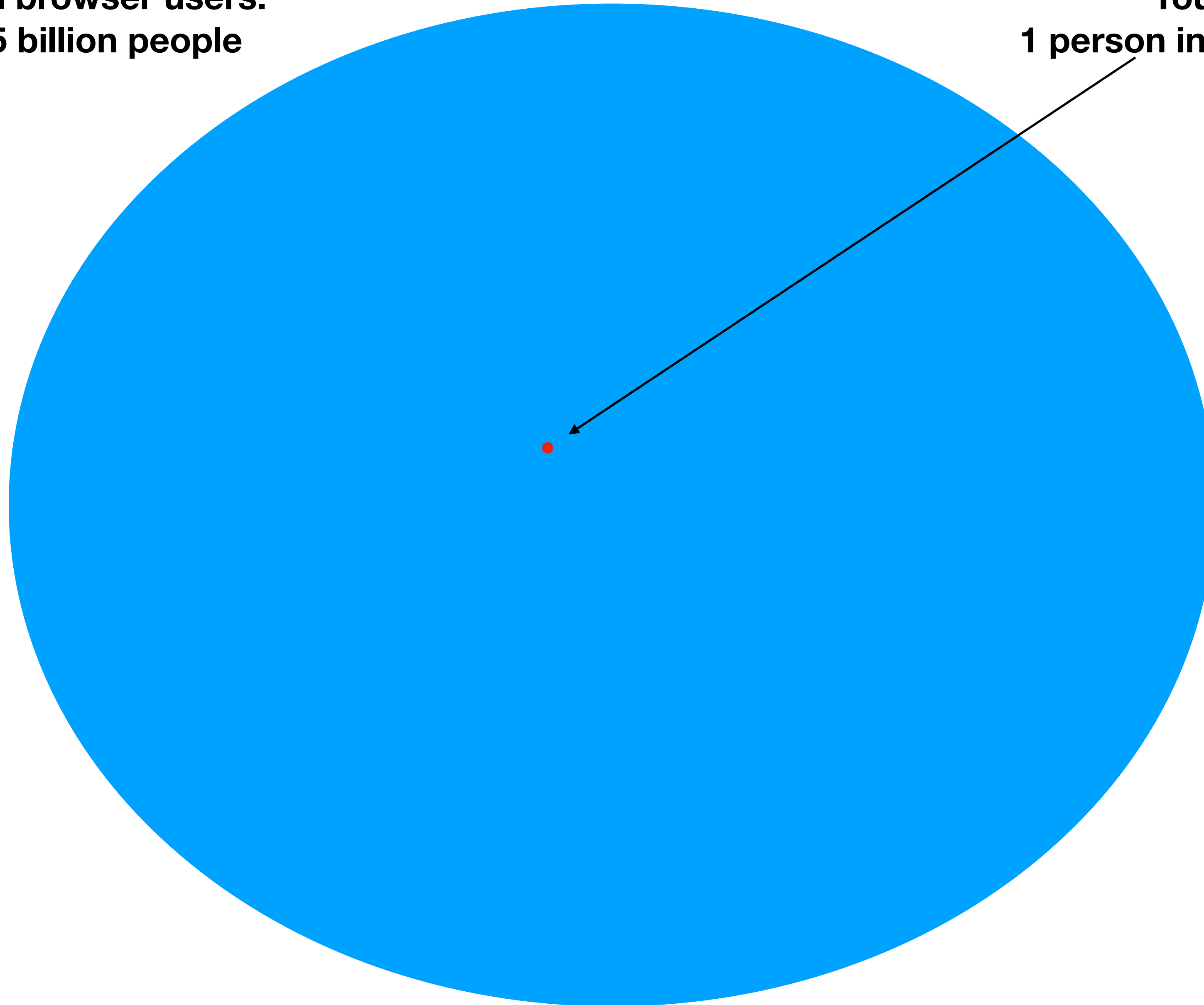
- **Large number of semi-identifiers**
 - Browser size
 - Extra fonts
 - Audio hardware
 - Video hardware
 - Installed plugins
 - Color depth
- **Add the semi identification up...**

All browser users

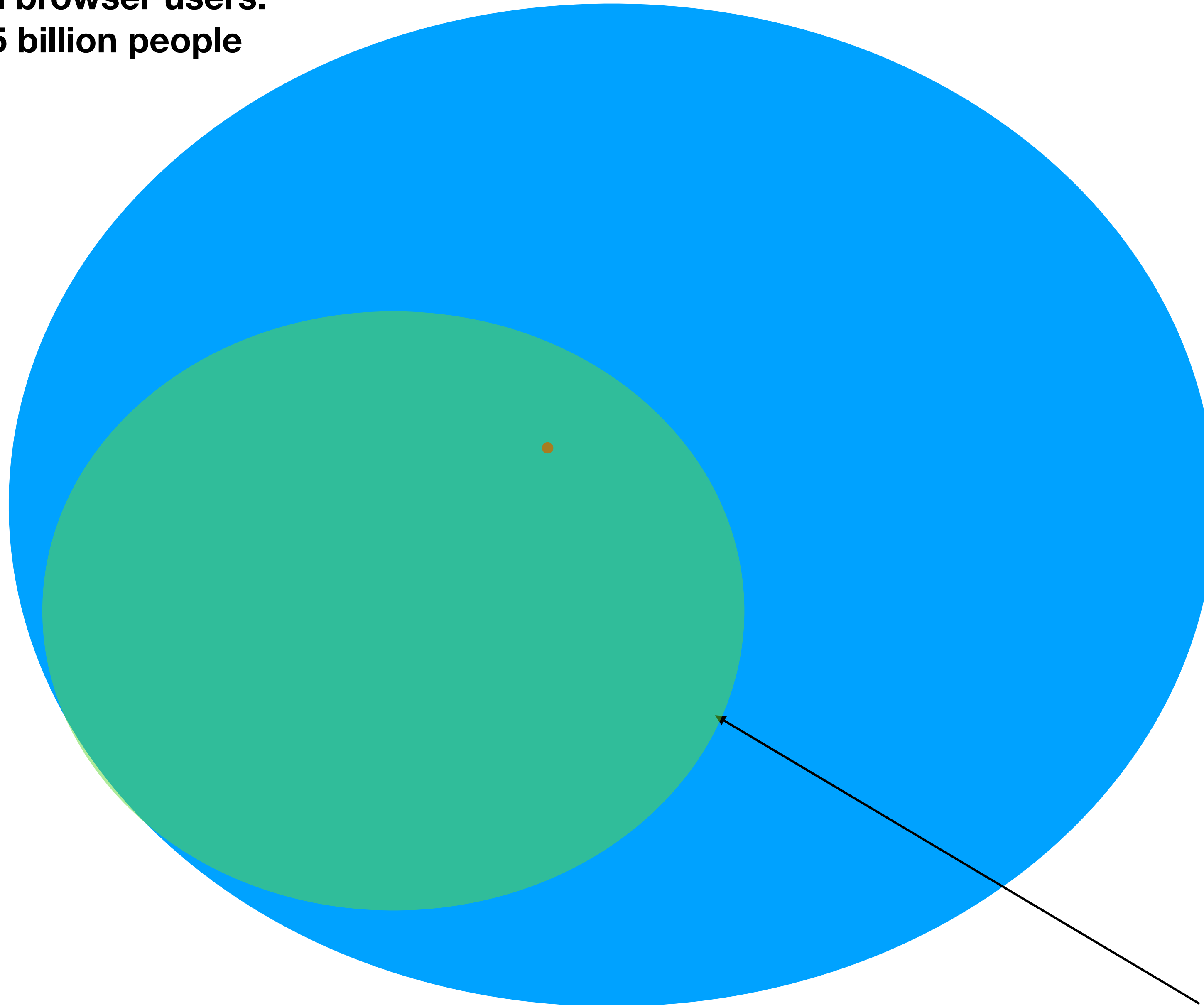


**All browser users:
5 billion people**

**You
1 person in 5 billion**

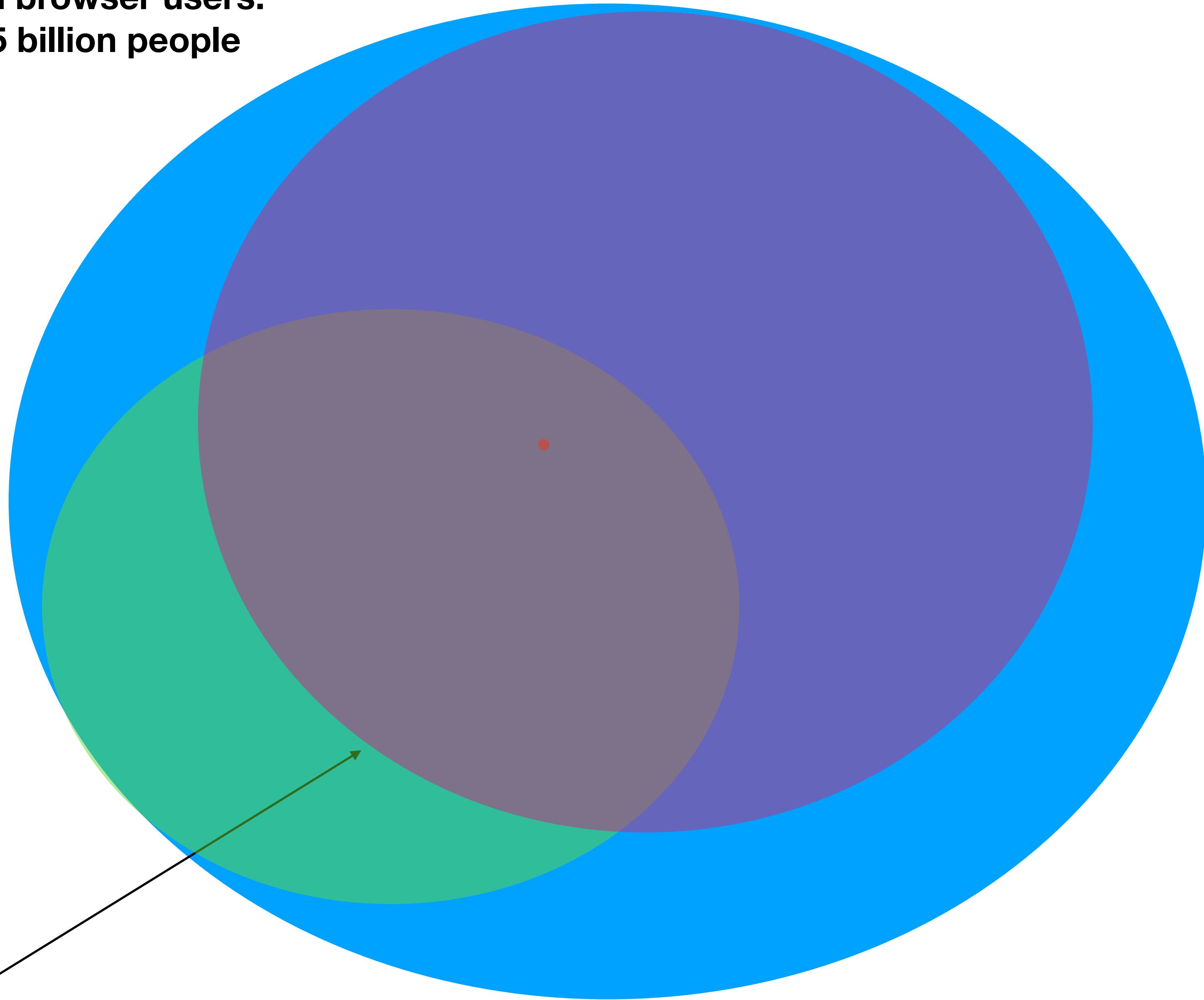


**All browser users:
5 billion people**



**Firefox
Users**

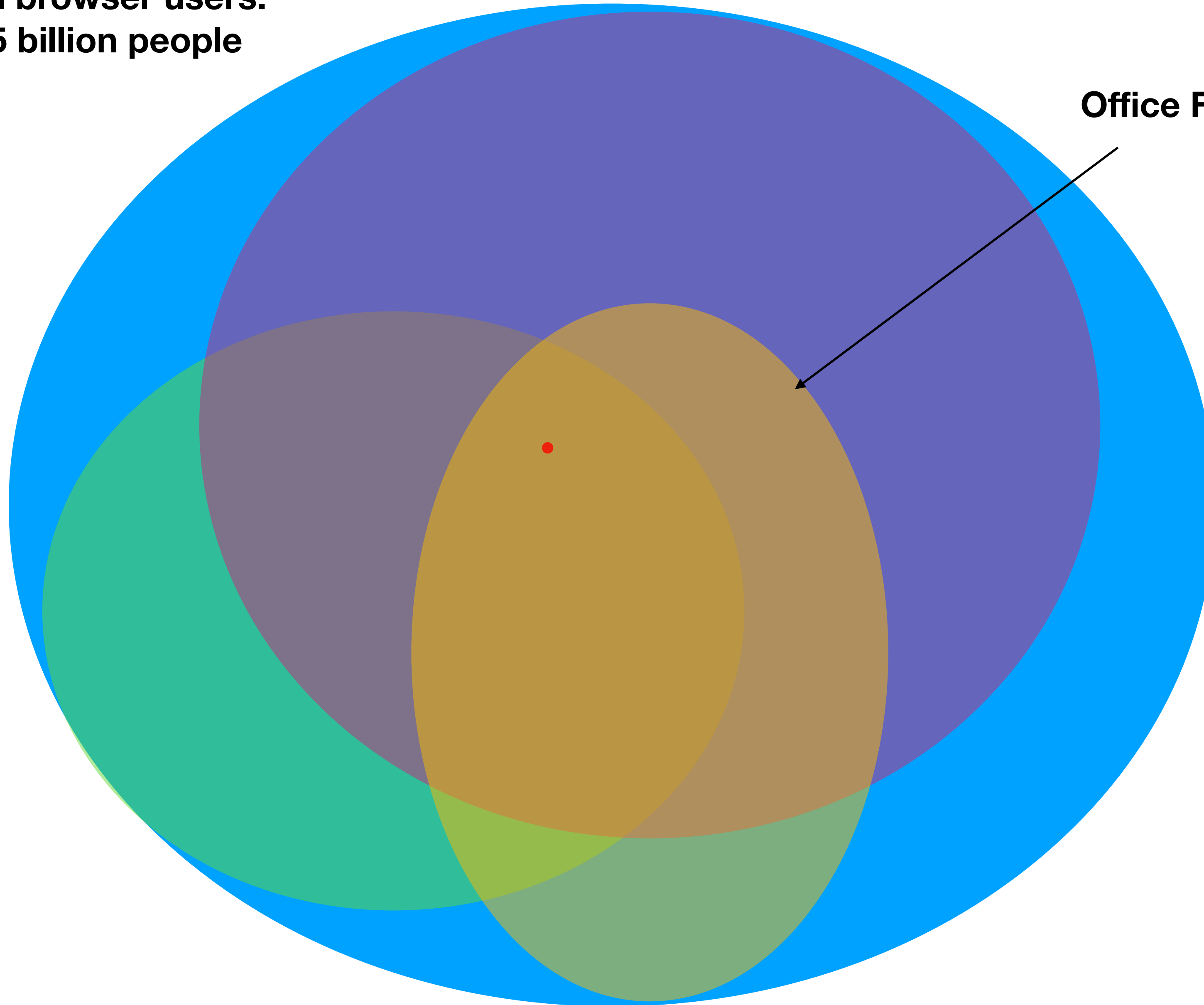
**All browser users:
5 billion people**



Windows users

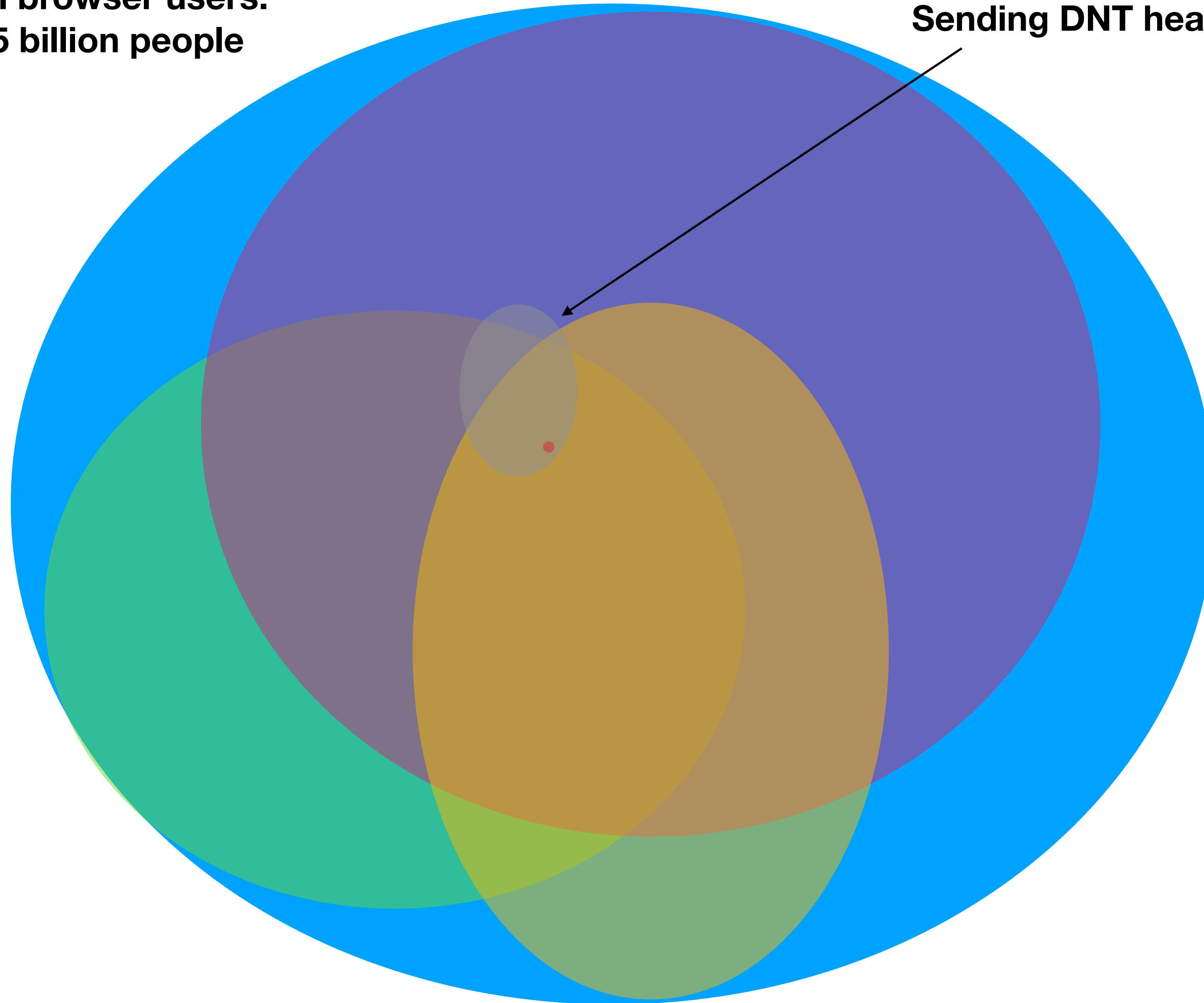
**All browser users:
5 billion people**

Office Fonts



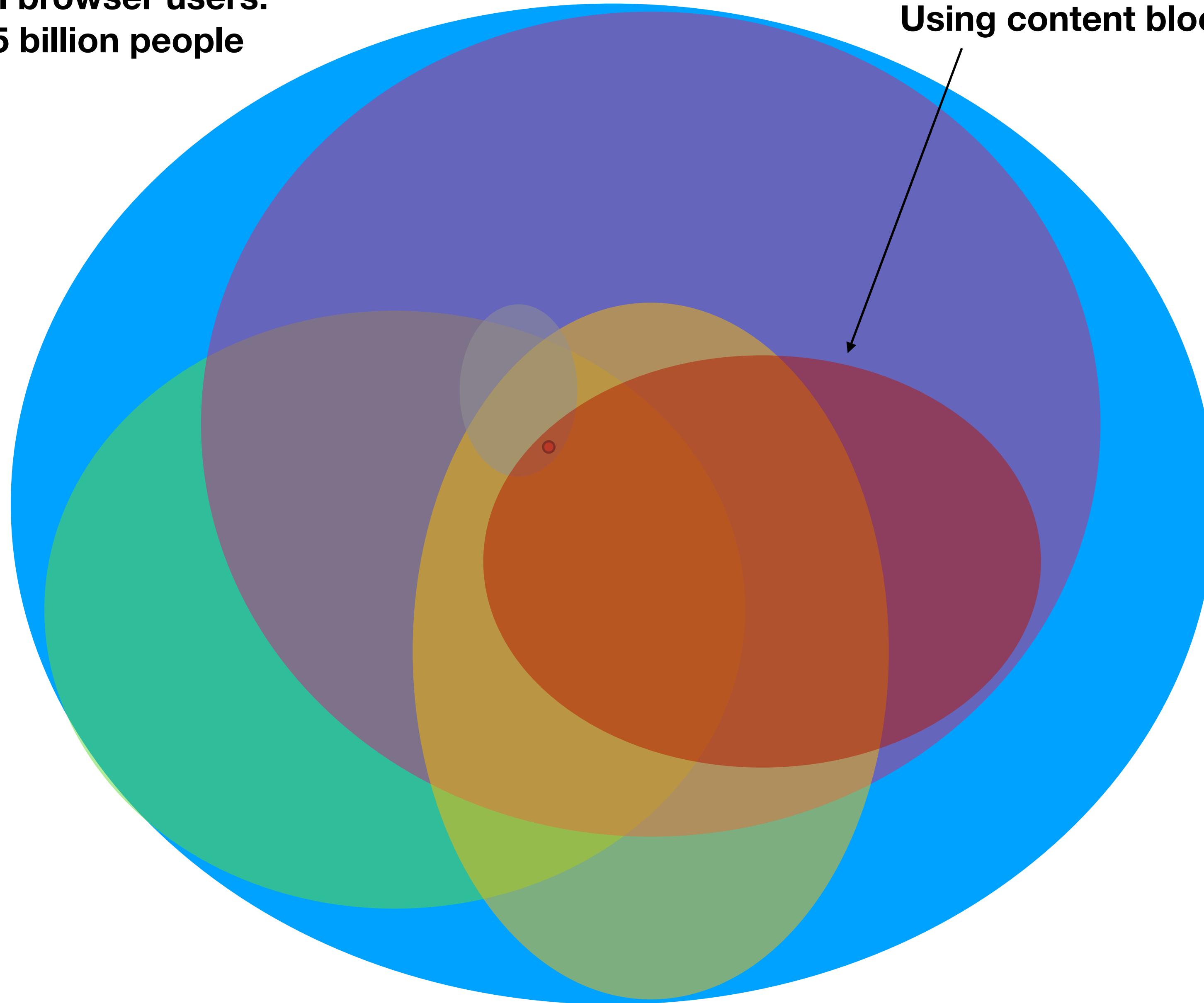
**All browser users:
5 billion people**

Sending DNT header



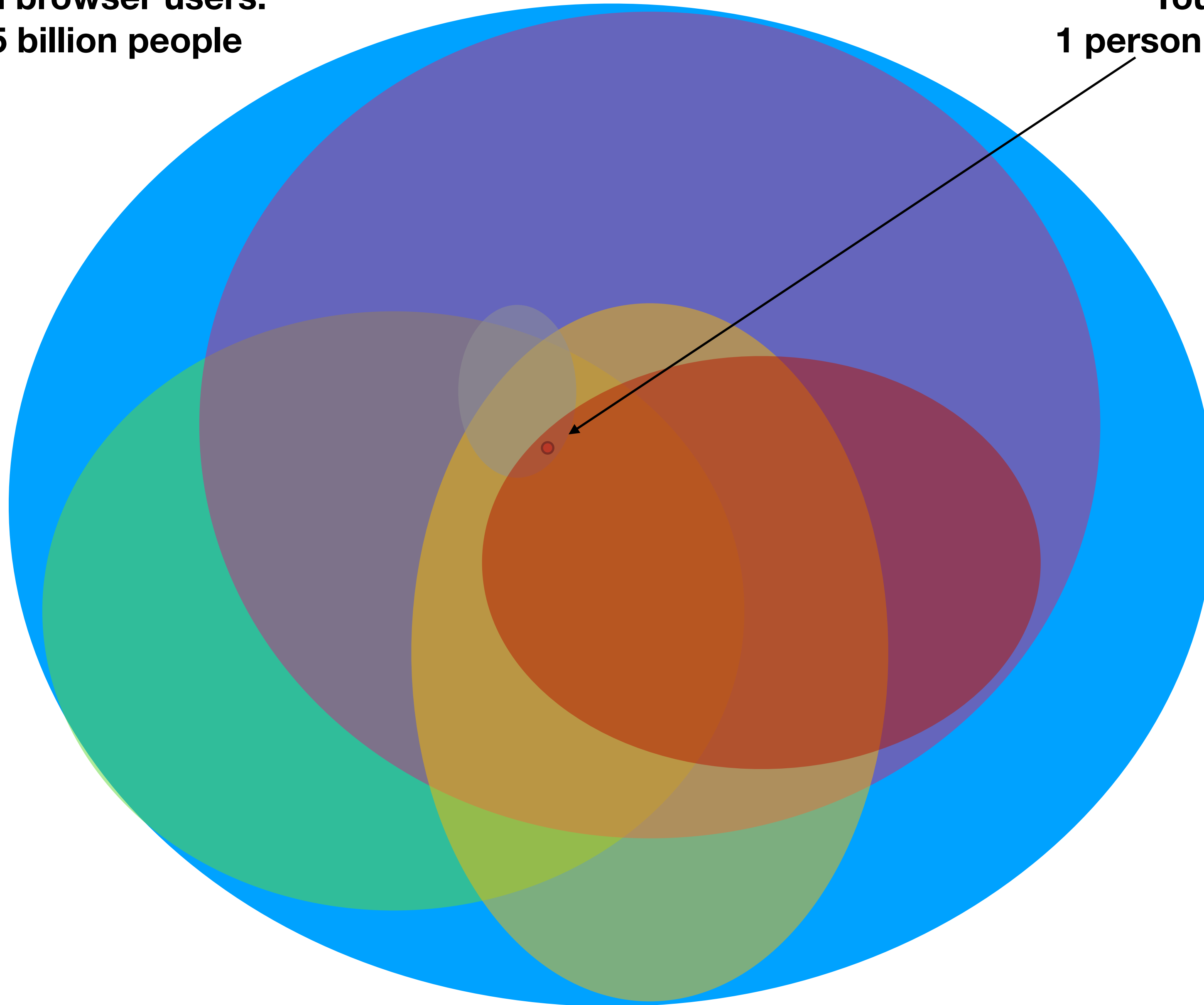
**All browser users:
5 billion people**

Using content blocker



**All browser users:
5 billion people**

**You
1 person in 100**




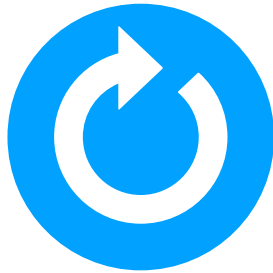



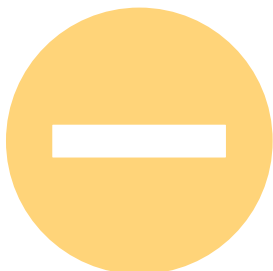
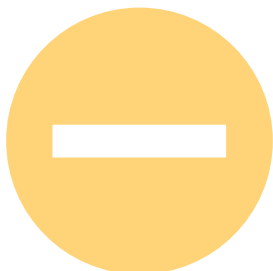
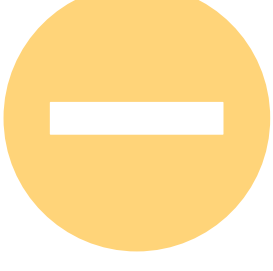

Fingerprinting, abstracted

- **Still needs a common value across boundaries**
Sites, sessions, time, etc
- **Value needs to be unique**
Otherwise it mixes you up with others
- **Value needs to be consistent**
Otherwise it doesn't (re)identify you

Possible Defenses

- **Try to make browsers look similar**
Reduce the “bits” available to fingerprinters
- **Try to block bad parties**
Keep the “bad folks” out
- **Privacy budgets**
Only allow sites to do so much identifying, e.g., 10 bits but not more
- **Randomization**
Make browser look intentionally different, within each boundary

Fingerprinting: Defenses

	Chrome	Safari	Edge	Firefox	Brave
Restricted hardware					
Feature selection / removal					
Block fingerprinters					
Randomization					

Tracking Techniques


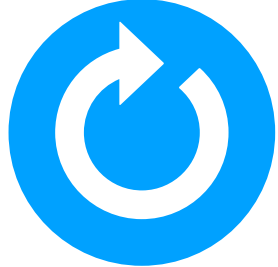

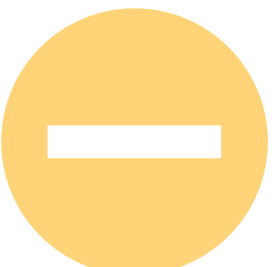
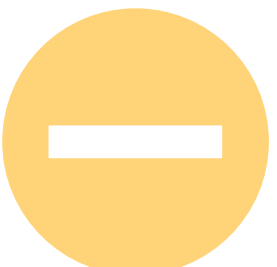
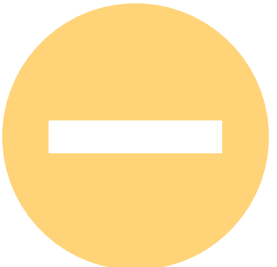
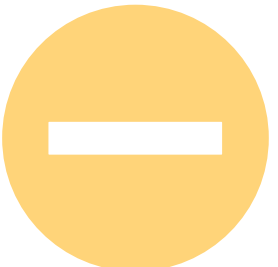
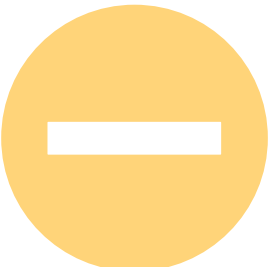

- Third-party DOM storage
- Network state
- Bounce tracking
- Browser fingerprinting
- IP address
- Personal identifiers



IP Addresses are pretty unique!

- **...especially if you look for clusters**
The 3 ips you most commonly connect from is very unique
- **IPv6 makes it a lot worse**
Obviously... :-/
- **Four general approaches**
 - Contracts / promises
 - proxies
 - mix nets
 - block bad parties

IP Addresses Defenses

	Chrome	Safari	Edge	Firefox	Brave
Websites promise					
Proxies		Private relay 		Optional VPN 	Optional VPN 
Mix networks					Optional Tor 
Block bad parties					

Tracking Techniques

- Third-party DOM storage
- Network state
- Bounce tracking
- Browser fingerprinting
- IP address
- Personal identifiers







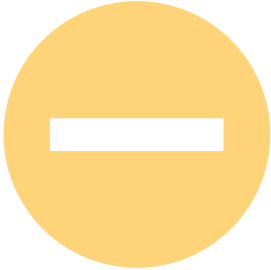
Personal Identifiers

- **Names, email addresses, CCN, etc**
“old school”
- **Can be combined with offline sources**
Credit agencies, public legal records, tax documents, etc
- **Baked into the web**
Authentication, user accounts, etc

Partitioning to the Rescue (?)

- **User holds the “true” value**
e.g., true email address
- **Browser holds a secret**
e.g., `secret = rand()`
- **Derive per site identities**
e.g. `hash(email + secret + eTLD+1) + @private-email.com`
- **Applicable to a range of identifiers**
Email, CCN, Crypto addresses

Personal Identifiers: Defenses

	Chrome	Safari	Edge	Firefox	Brave
Partition email					
Partition Web3					
Block scripts					

Overview

- **Why Privacy Matters**
A sloppy manifesto
- **Defining Tracking**
Abstracting the problem
- **Tracking in Practice**
Methods and defenses
- **Privacy Beyond Tracking**
Other issues and concerns



Privacy is more than Absence of Tracking

- **Browsers shouldn't share information unless its helpful to user**
e.g., FLoC
- **Browsers should serve users first and exclusively**
e.g., Reporting API, FLEDGE
- **Browsers shouldn't introduce capabilities that remove user choice**
WebBundles
- **Browsers shouldn't confuse users!**
First-party sets, SXG
- **First-parties are suspect too...**

Other privacy protections

- **Governments increasingly provide legal protections**
GDPR, CCPA, etc
- **Browsers can help users assert their privacy rights**
e.g., GlobalPrivacyControl
- **Authored by activists, academics, New York Times, DuckDuckGo, Brave**
Implemented in Brave and DDG
- **Beware of conflating with “consent management” systems**

A final plea...

- You are all plainly, amazingly smart people
- You'll be able to (mostly) choose your job
- Privacy harms are particularly difficult to remediate
- Consider the privacy implications of a job before you take it

A final plea...

- You are all plainly, amazingly smart people
- You'll be able to (mostly) choose your job
- Privacy harms are particularly difficult to remediate
- Consider the privacy implications of a job before you take it

Thanks!