CSE 484/M584: Computer Security (and Privacy)

Spring 2025

David Kohlbrenner
dkohlbre@cs

UW Instruction Team: David Kohlbrenner, Yoshi Kohno, Franziska Roesner, Nirvan Tyagi. Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials

Admin

- Lab 3 Weblab due next week.
  - Start early, etc etc
- Please double check your Lab 2 gradescope handins
  - Partner status for code, etc.
  - Remember that you need to make sure there is ONE handin for partners.

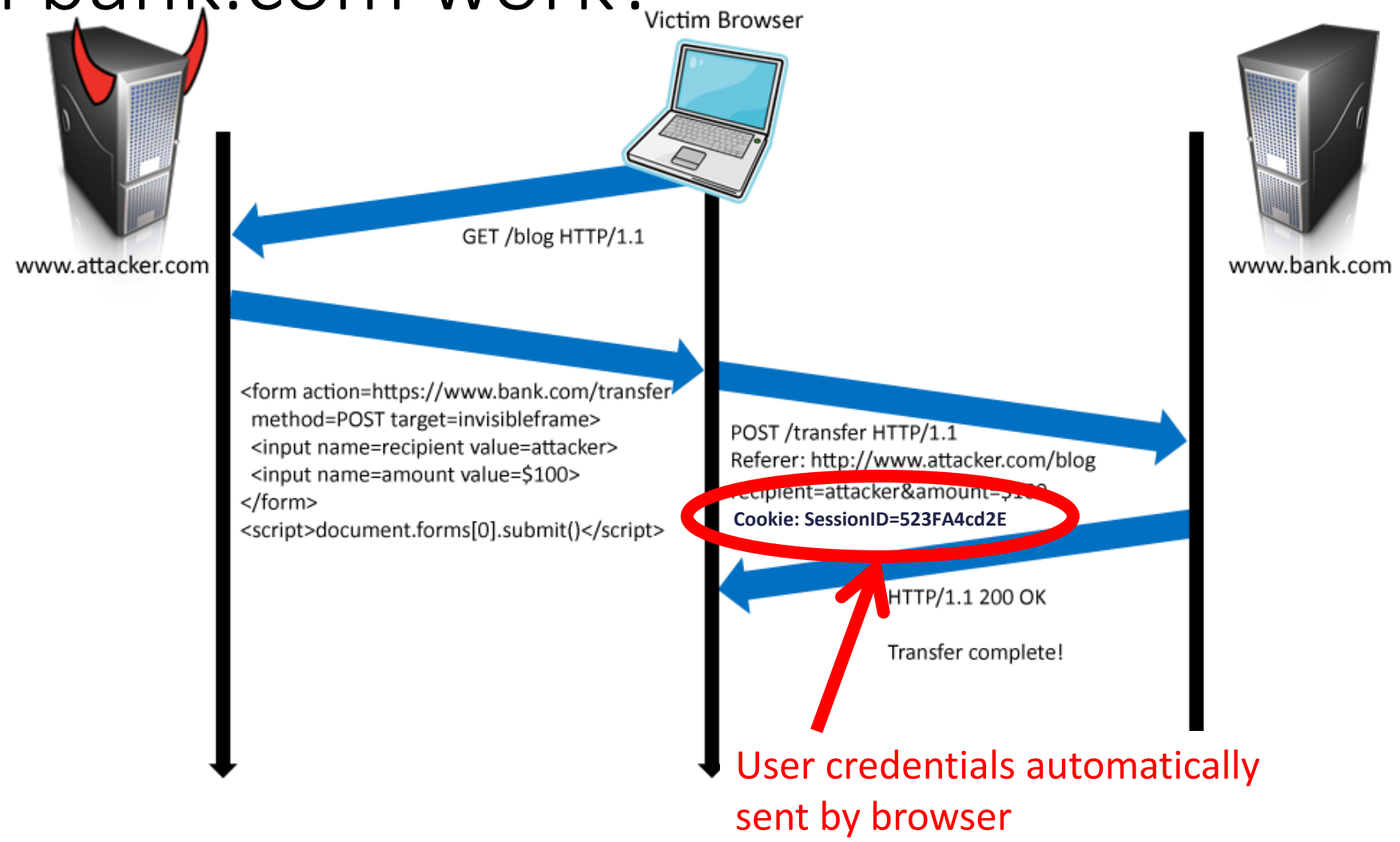
genai

- No really, please don’t use this.

CSRF

Its just one POST request, how bad can it be?

Why does adding a magic value to the form from bank.com work?



Add Secret Token to Forms

```
<input type=hidden value=23a3af01b>
```

- "Synchronizer Token Pattern"
- Include a secret challenge token as a hidden input in forms
  - Token often based on user's session ID
  - Server must verify correctness of token before executing sensitive operations
  - OR add it as an additional cookie, with different permissions (which ones?)
- Why does this work?
  - **Same-origin policy:** attacker can't read token out of legitimate forms loaded in user's browser, so can't create fake forms with correct token

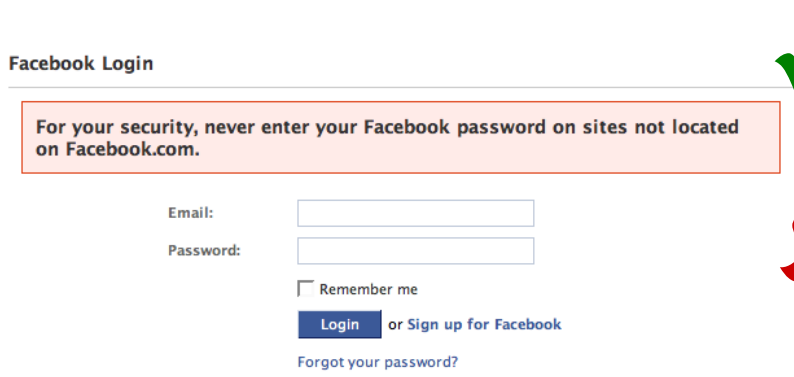
CSRF Defenses

Relevant and useful discussion: https://github.com/golang/go/issues/73626

- Double-submit
  - magic token in POST (and the cookie)
- Origin headers/refer[r]er checking:
  - Validate what the browser says about the request originating from
  - Pre-2020, some browsers didn't send on POST(??)
- Cookie restrictions (SameSite)
  - Tells browser not to send cookies unless starting page is same origin (ish)
- Etc.

- Honestly, go read filippo's golang discussion, its great.

Referer Validation



✓ Referer:
http://www.facebook.com/home.php

✗ Referer:
http://www.evil.com/attack.html

? Referer:

- Lenient referer checking – header is optional
- Strict referer checking – header is required

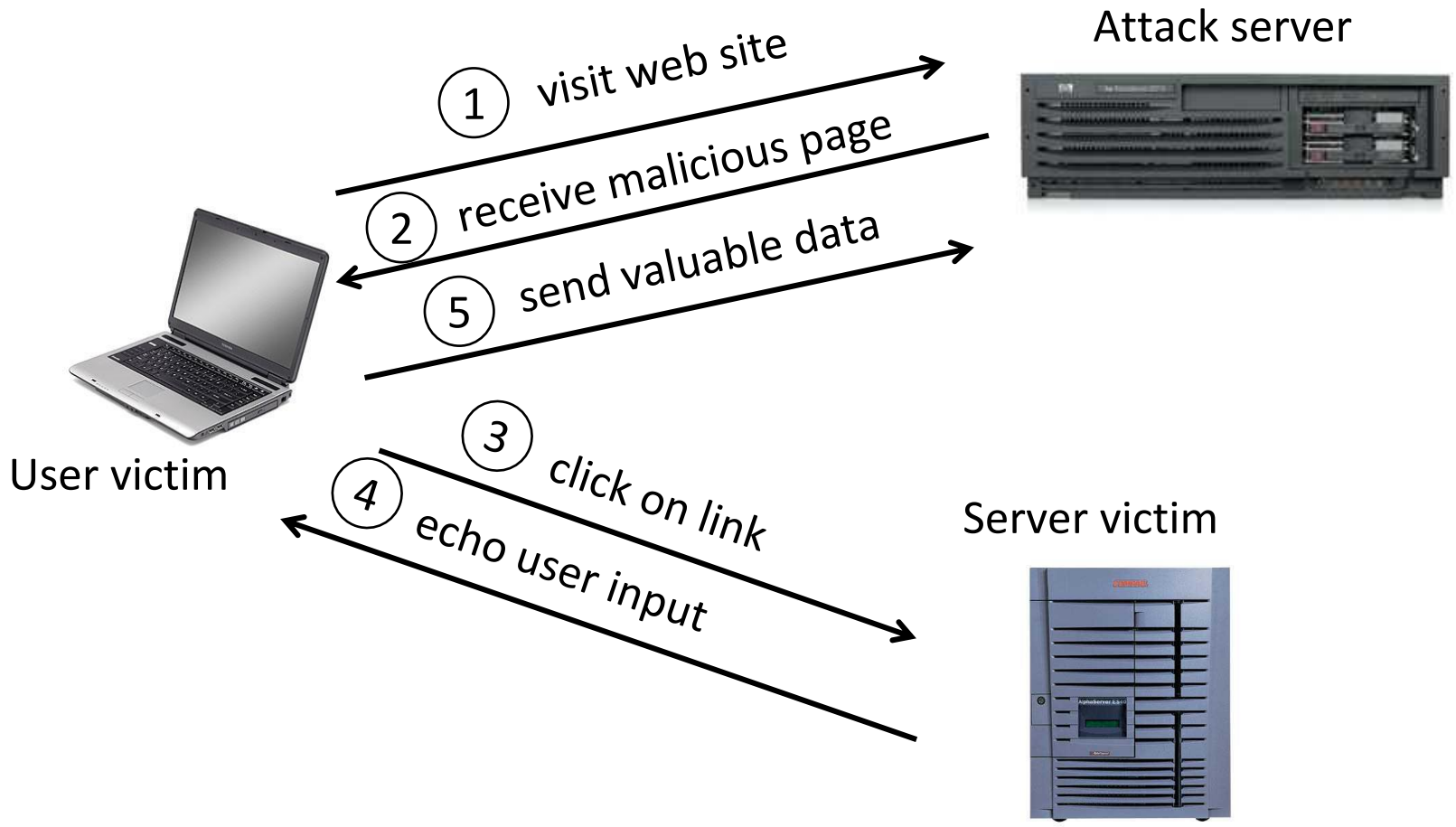
Why Not Always Strict Checking?

- Why might the referer header be suppressed?
  - Stripped by the organization's network filter
  - Stripped by the local machine
  - Stripped by the browser for HTTPS $\rightarrow$ HTTP transitions
  - User preference in browser
  - Intentional browser behaviors
  - etc

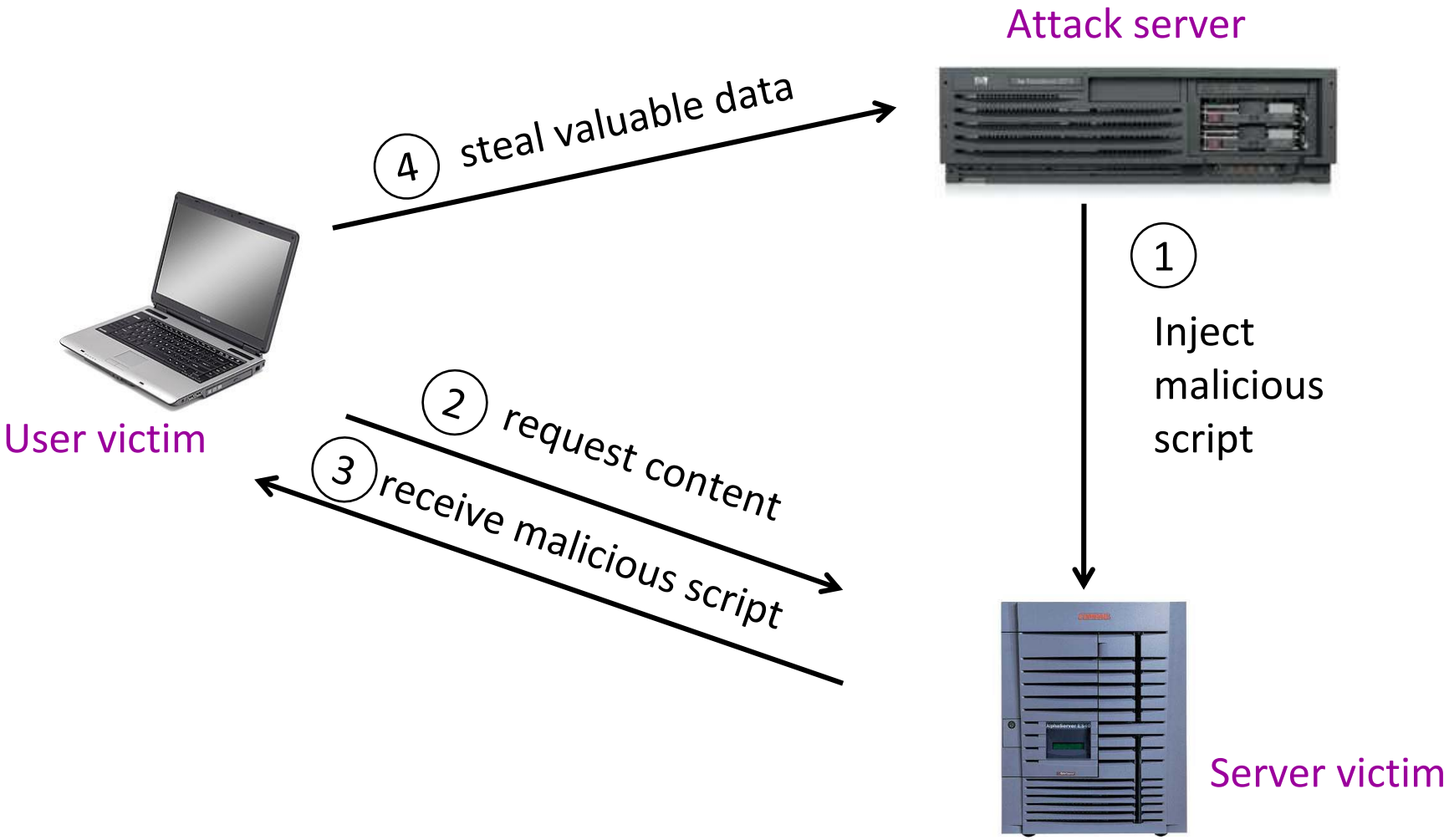
Surprise not-quiz time

XSS again

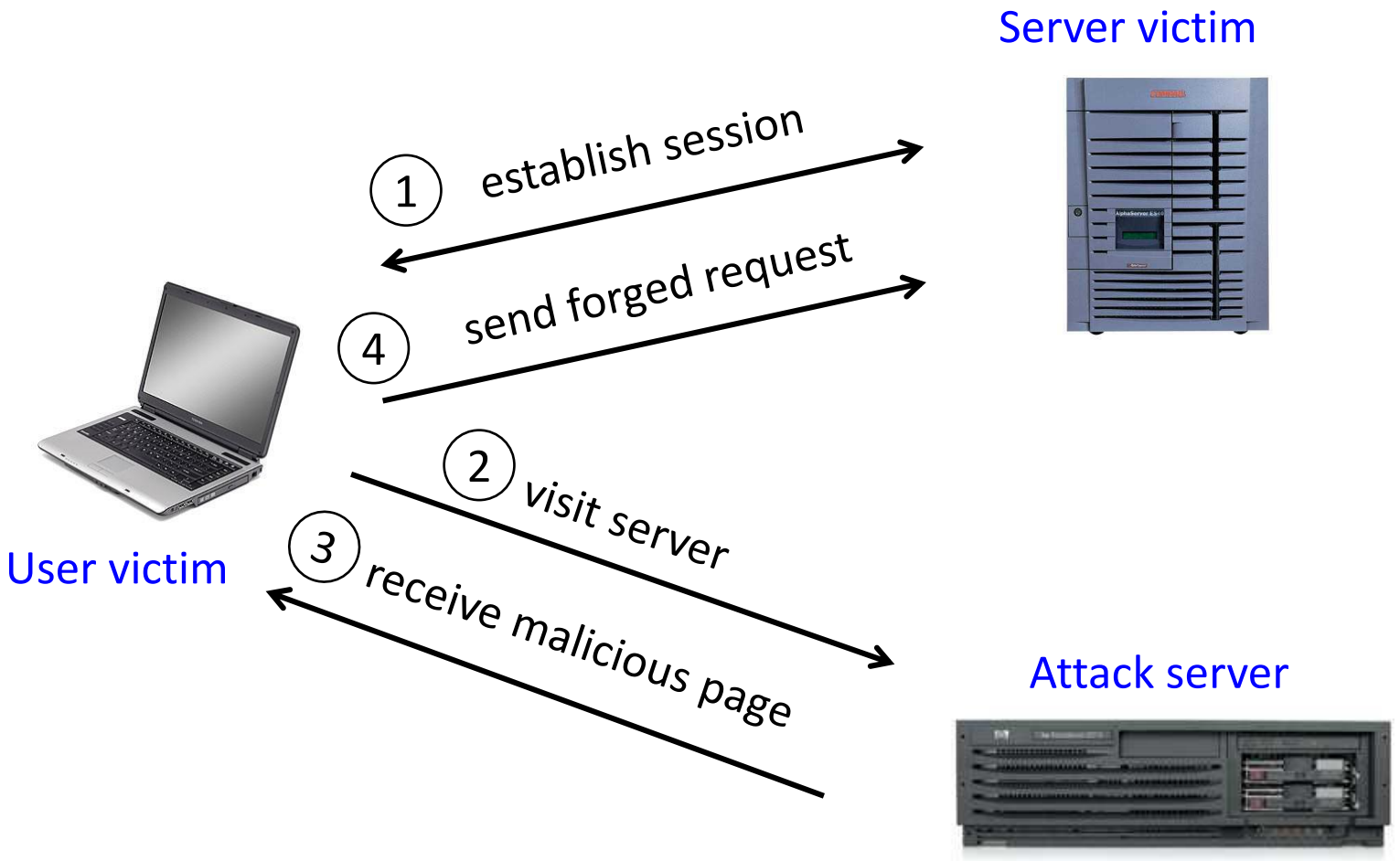
Reflected XSS



Stored XSS


Attack server
4 steal valuable data
1
Inject malicious script
2 request content
3 receive malicious script
User victim
Server victim

XSRF (aka CSRF)



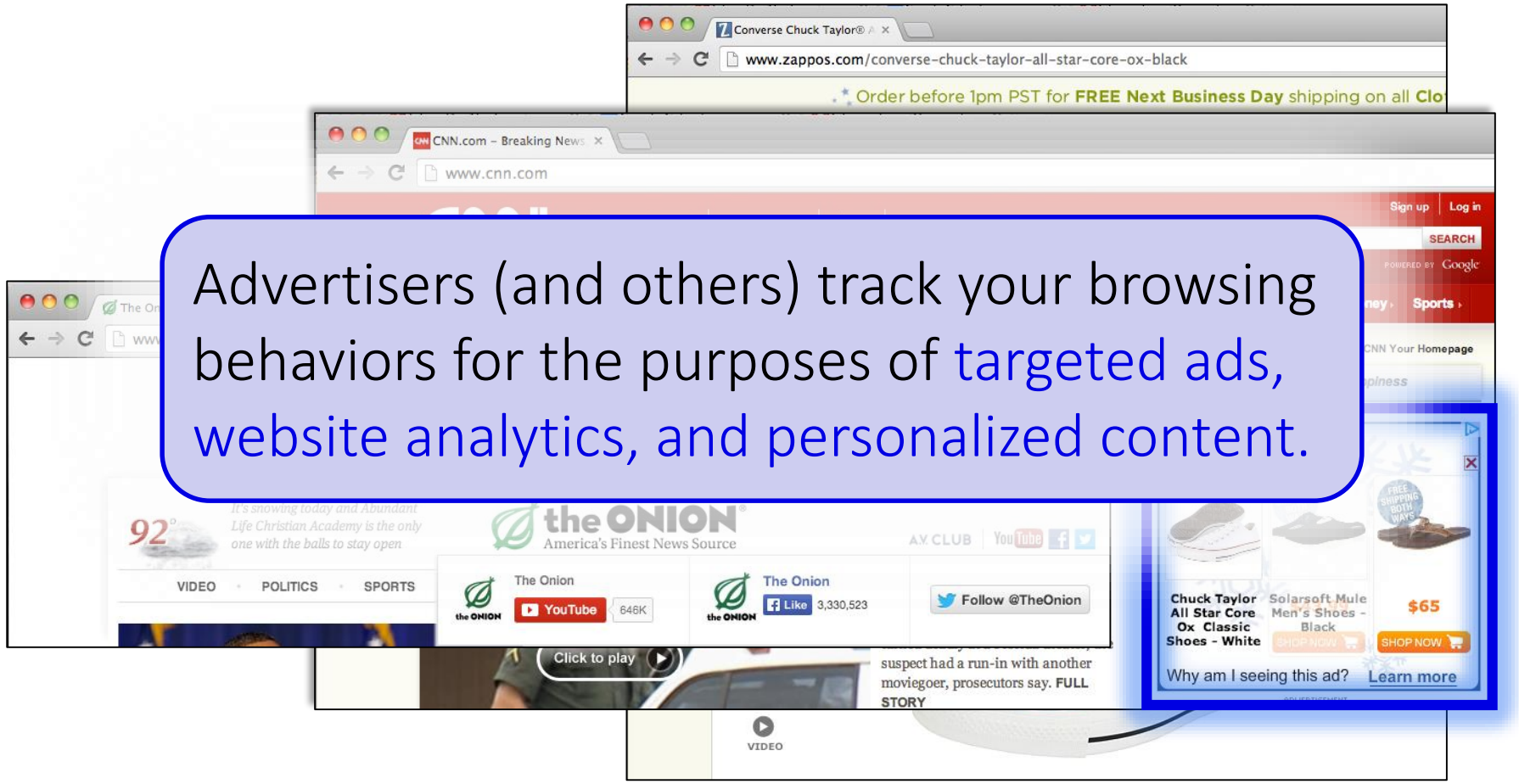
Privacy and web tracking

Aka: so what were all those cookies for anyway?

A topic in flux

- Tracking via cookies
- Tracking via other methods
- Fingerprinting

Ads That Follow You



Third-Party Web Tracking

These ads allow **criteo.com** to link your visits between sites, even if you never click on the ads.

Gradescope

- Do you take any particular precautions about tracking?
  - For web browsing?
  - Phone apps?
  - Phone tracking?

- Why do you take or not take those actions?
  - Any you would like to but don’t?

chiefmartec.com April 2020

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

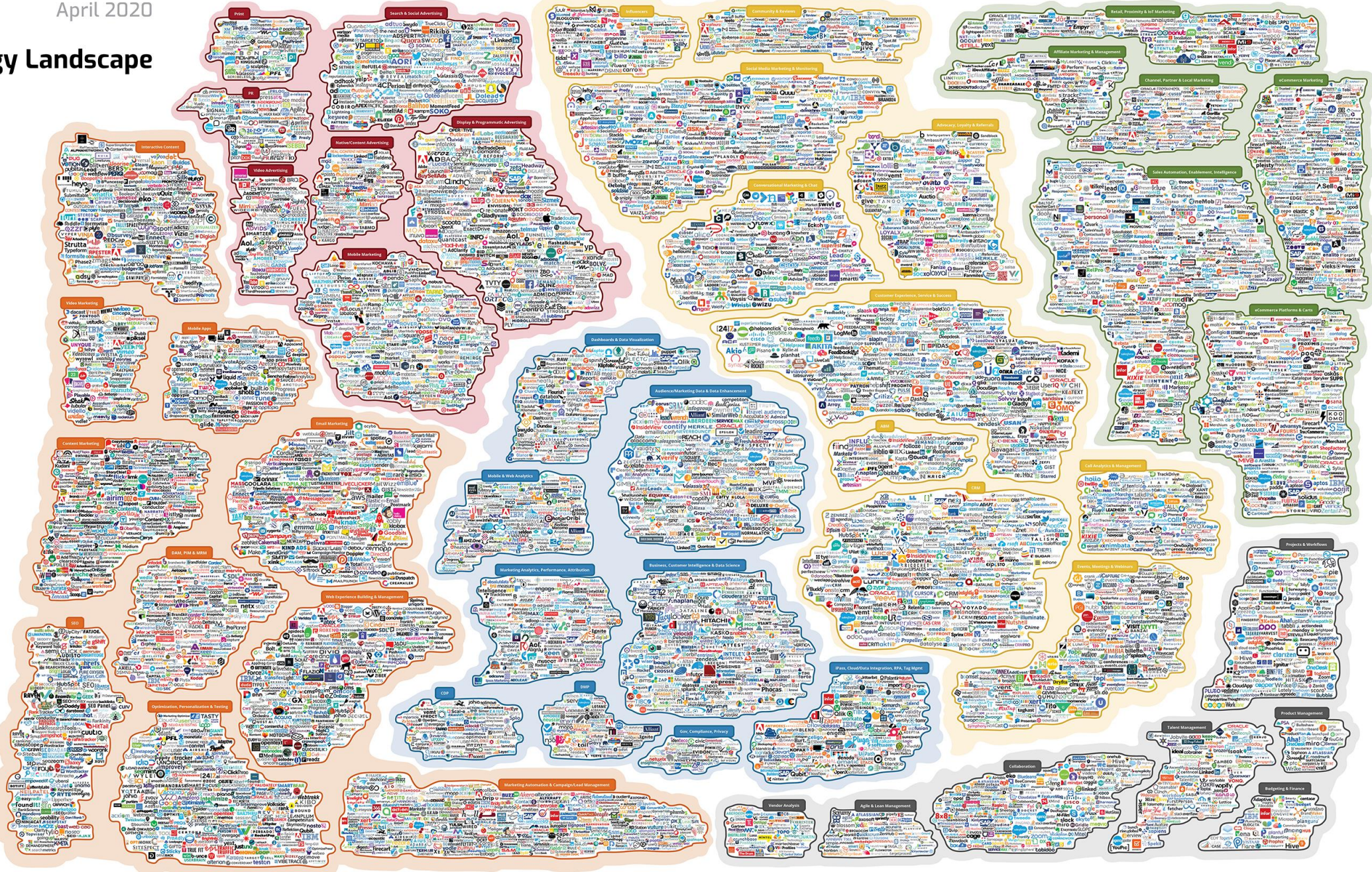
2018
6,829 solutions

2017
5,381 solutions

2016
3,874 solutions

2015
1,876 solutions

2014
947 solutions



Produced by Scott Brinker (@chiefmartec) and Blue Green Brands (@bluegreenbrands).

MartechMap an initiative by chiefmartec & MartechTribe

2022 Marketing Technology Landscape May 2022

Advertising & Promotion

Display & Programmatic Advertising

Mobile Marketing

Native/Content Advertising

PR

Print

Search & Social Advertising

Video Advertising

Content & Experience

Content Marketing

CMS & Web Experience Management

DAM & MRM & PIM

Email Marketing

Interactive Content

Marketing Automation & Campaign/Lead Management

Mobile Apps

Optimization Personalization & Testing

SEO

Video Marketing

Social & Relationships

ABM

Call Analytics & Management

Customer Experience Service & Success

Influencers

CRM

Advocacy Loyalty & Referrals

Community & Reviews

Events, Meetings & Webinars

Social Media Marketing & Monitoring

Live Chat & Chatbots

Commerce & Sales

Retail, Proximity & IOT

Affiliate Marketing & Management

Sales Automation Enablement & Intelligence

eCommerce Platforms & Carts

eCommerce Marketing

Channel Partner & Local Marketing

Data

Marketing Analytics Performance & Attribution

Audience/Marketing Data & Data Enhancement

Ipaas Cloud/Data Integration & Tag Management

Business/Customer Intelligence & Data Science

DMP

Dashboards & Data Visualization

Governance Compliance And Privacy

Mobile & Web Analytics

Customer Data Platform

Management

Agile & Lean Management

Collaboration

Talent Management

Budgeting & Finance

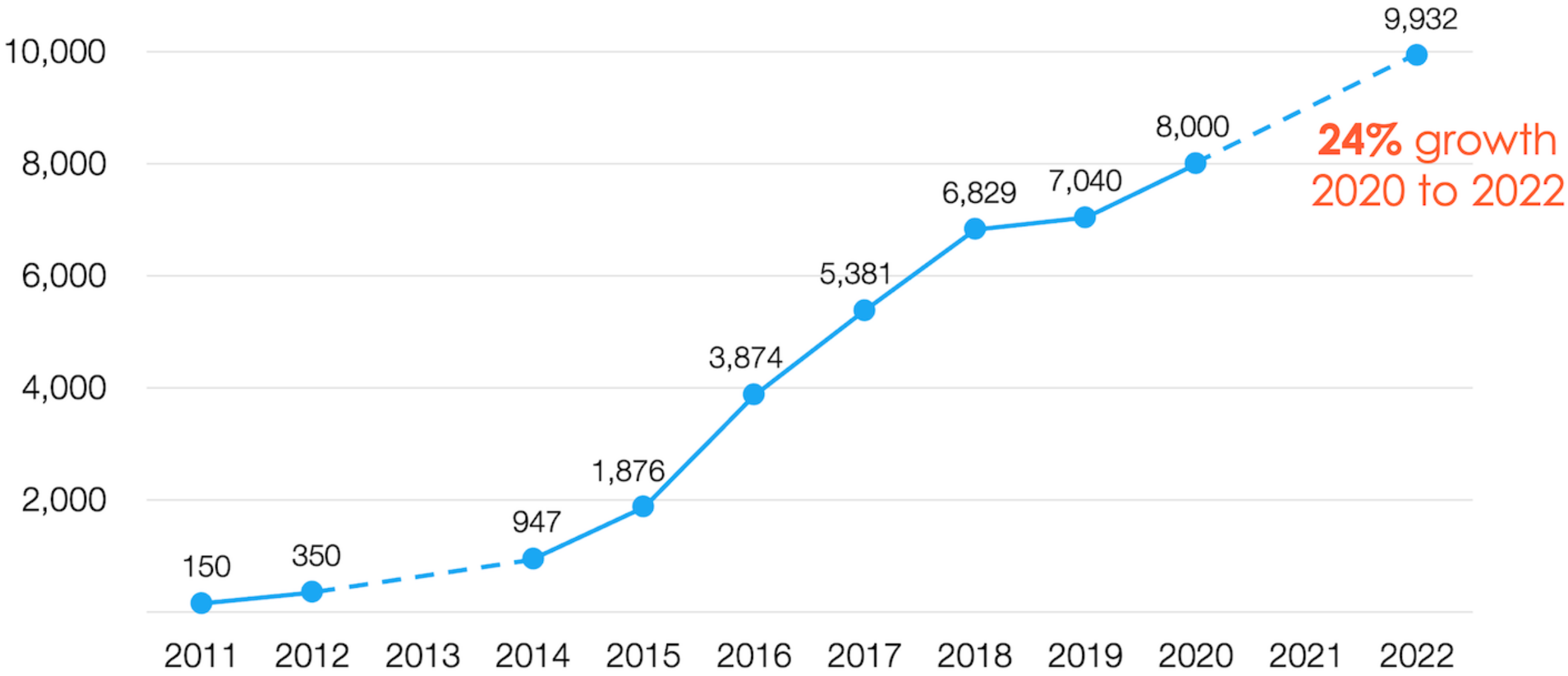
Projects & Workflow

Product Management

Vendor Analysis & Management

visit martechmap.com to search, sort & filter

6,521% growth 2011 to 2022

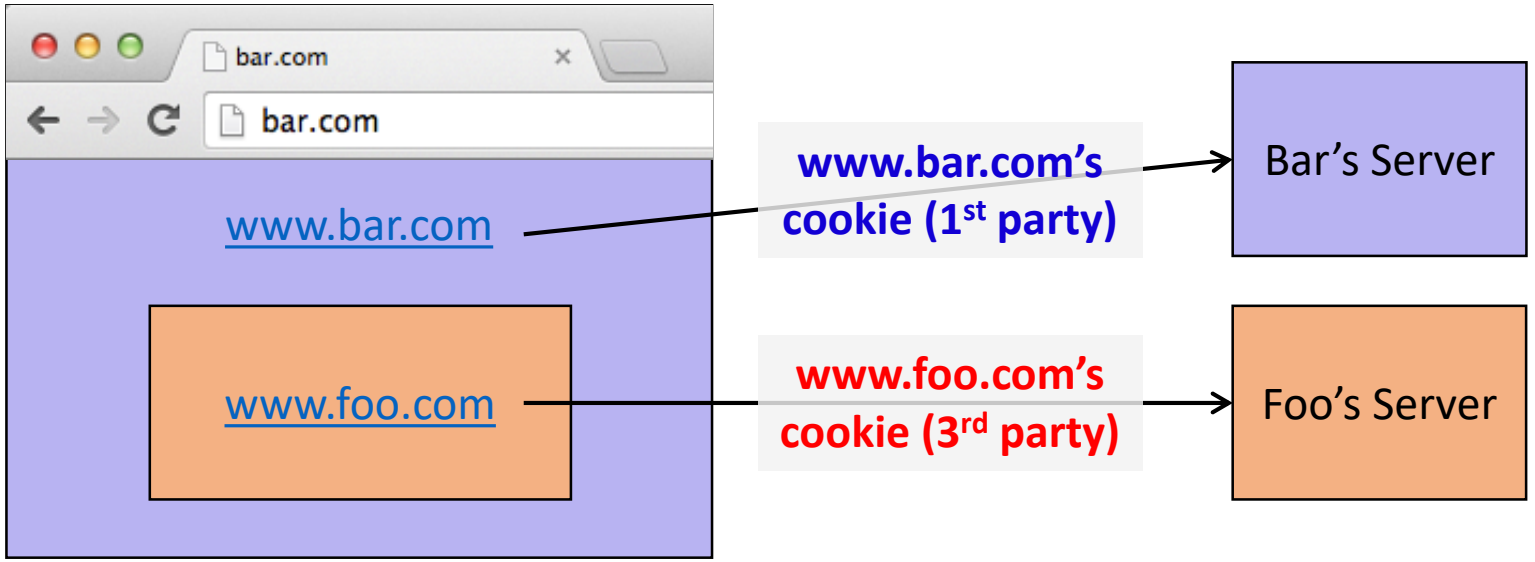


https://chiefmartec.com/2022/05/marketing-technology-landscape-2022-search-9932-solutions-on-martechmap-com/

Concerns About Privacy

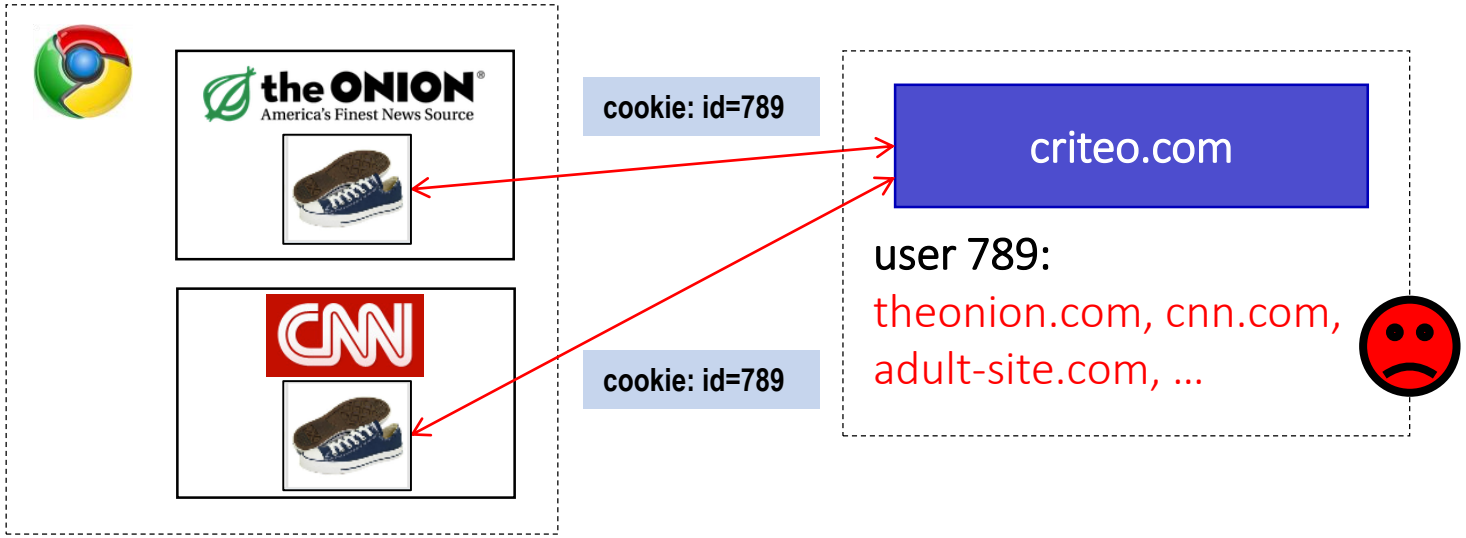
First and Third Parties

- First-party cookie: belongs to top-level domain.
- Third-party cookie: belongs to domain of embedded content (such as image, iframe).



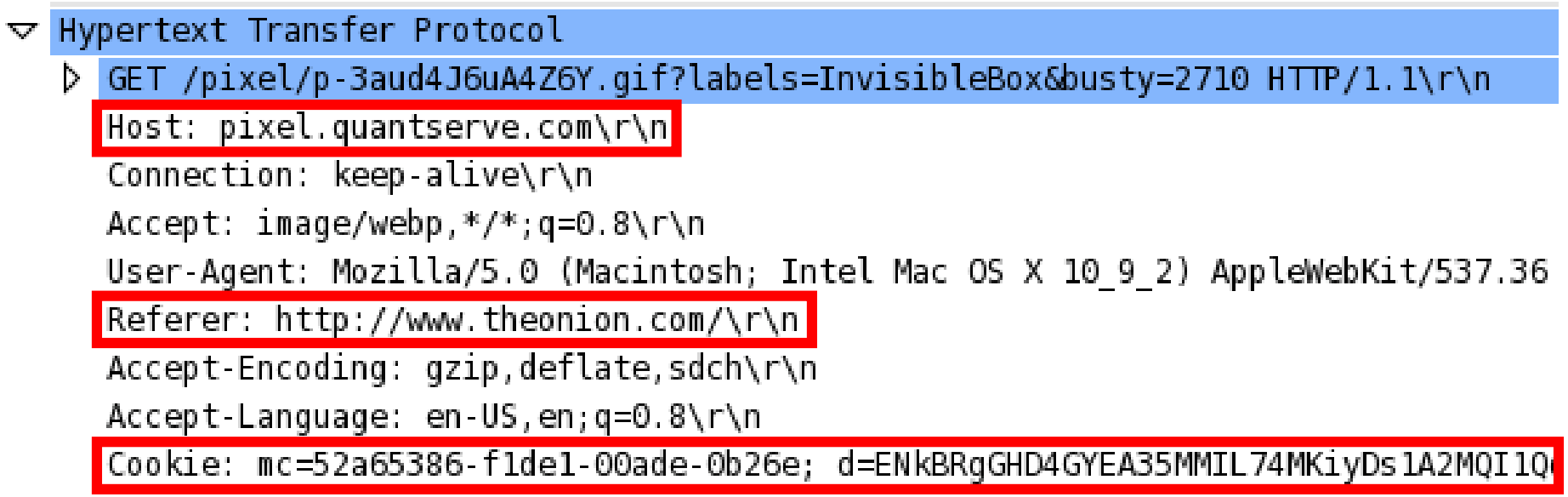
Anonymous Tracking

Trackers included in other sites use third-party cookies containing unique identifiers to create browsing profiles.



Basic Tracking Mechanisms

- Tracking requires:
  (1) re-identifying a user.
  (2) communicating id + visited site back to tracker.

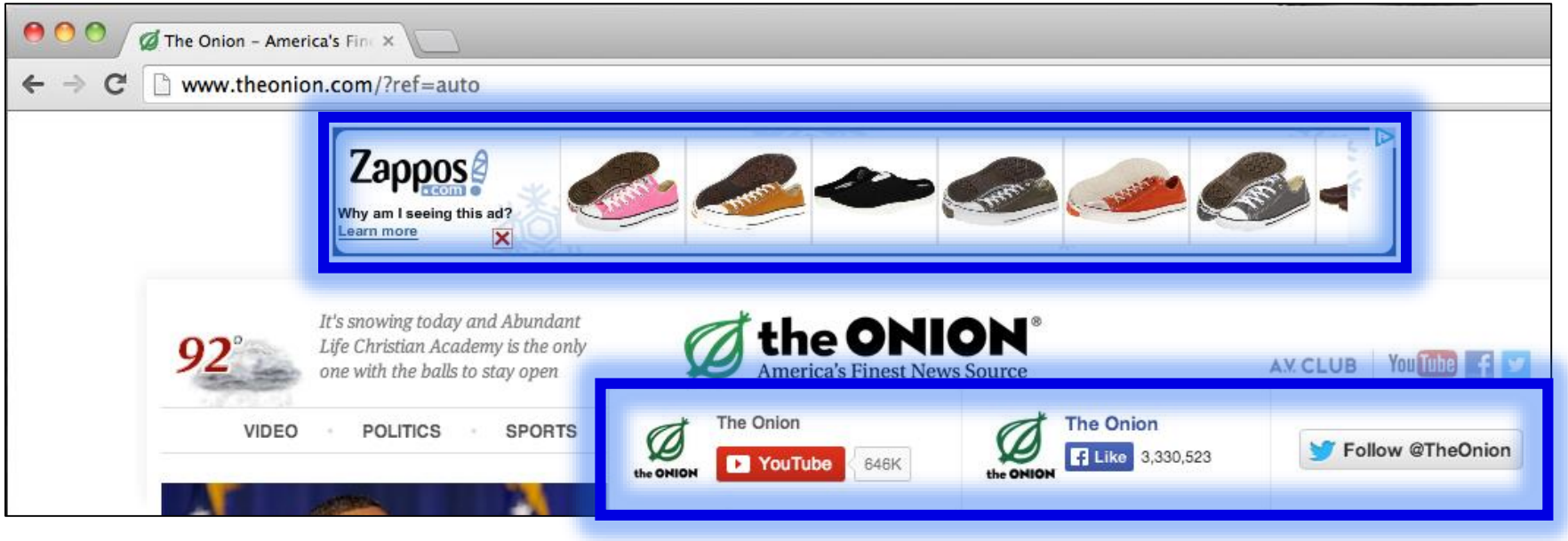


Tracking Technologies

- HTTP Cookies
- HTTP Auth
- HTTP Etags
- Content cache
- IE userData
- HTML5 protocol and content handlers
- HTML5 storage
- Flash cookies
- Silverlight storage
- TLS session ID & resume
- Browsing history
- window.name
- HTTP STS
- DNS cache

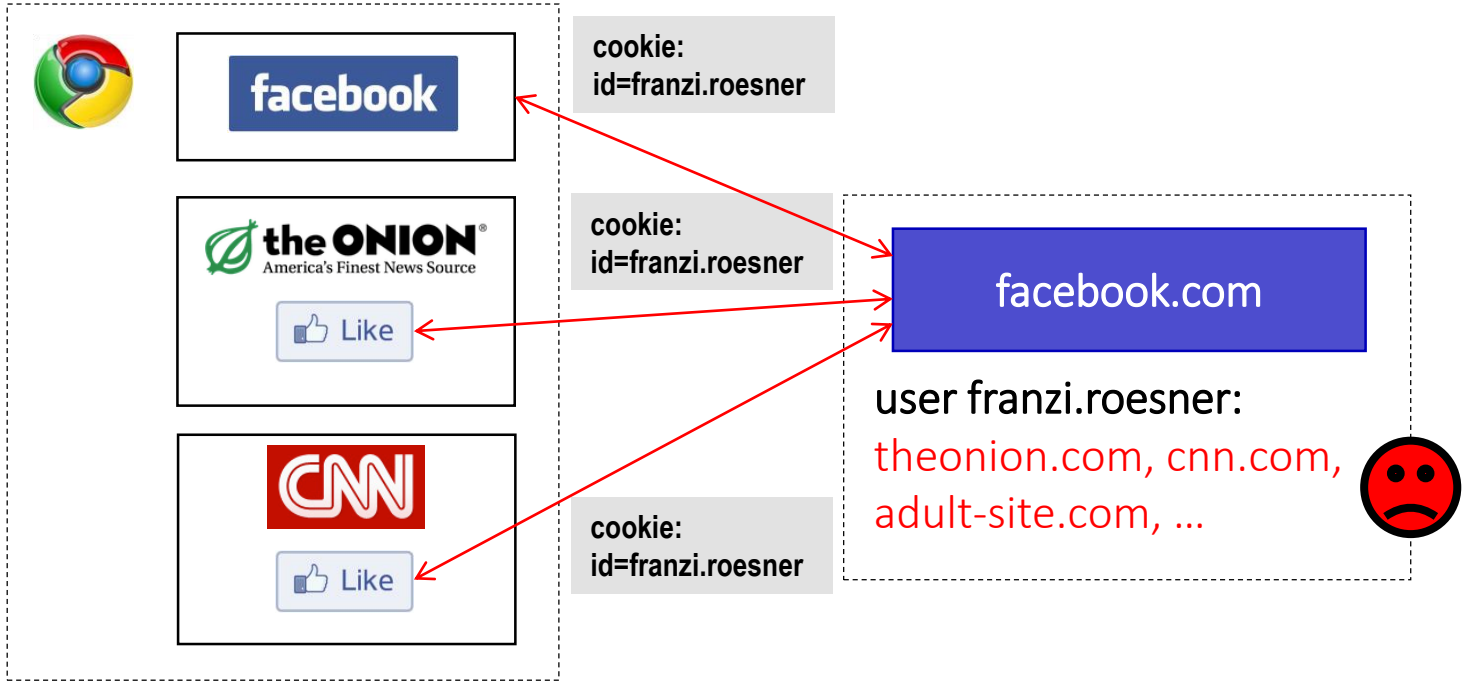
- "Zombie" cookies that respawn (http://samy.pl/evercookie)

Other Trackers?



"Personal" Trackers

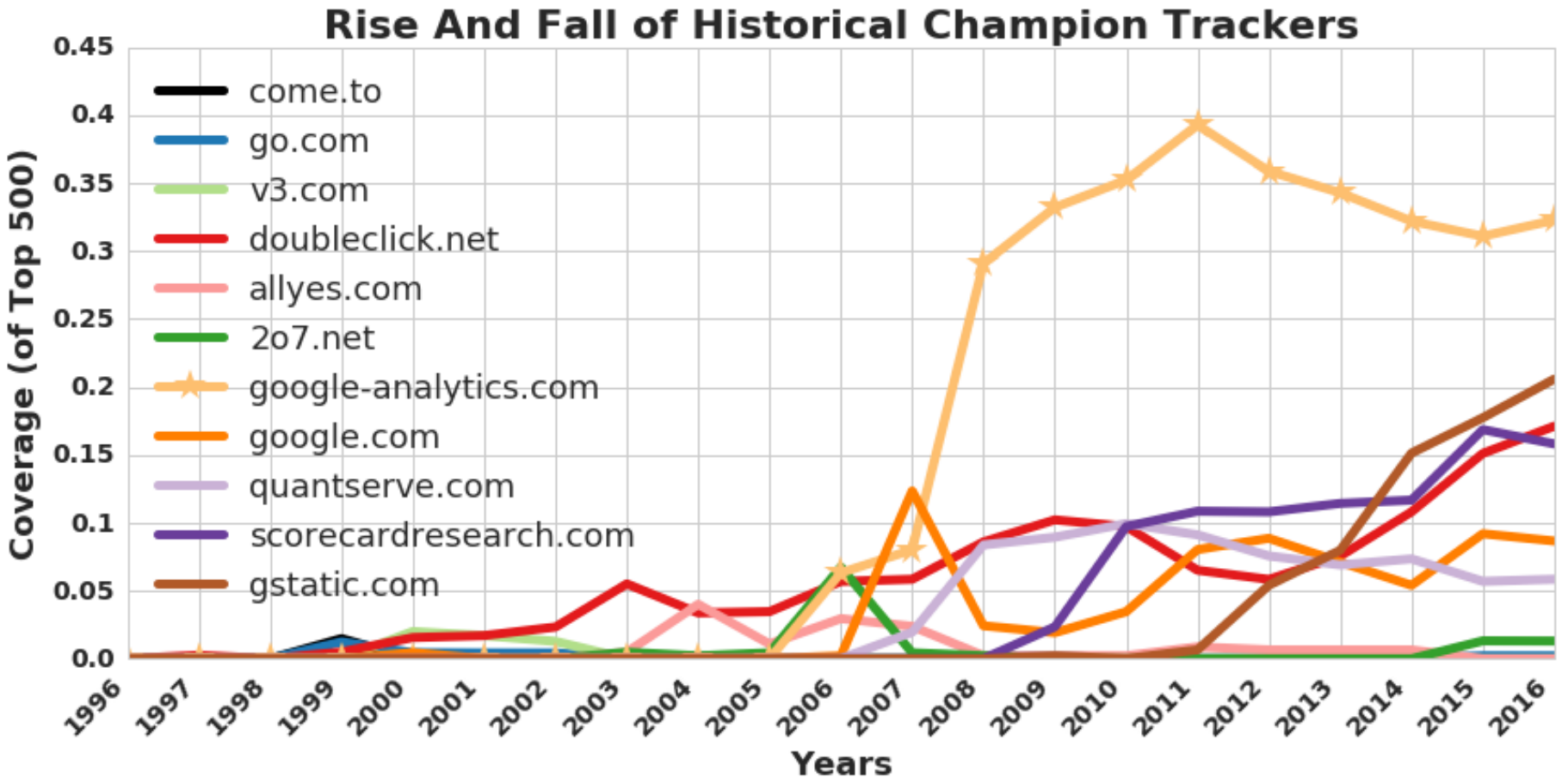
Personal Tracking



- Tracking is not anonymous (linked to accounts).
- Users directly visit tracker's site → evades some defenses.

1996-2016: More & More Tracking

- More trackers of more types, more per site, more coverage



Defenses to Reduce Tracking

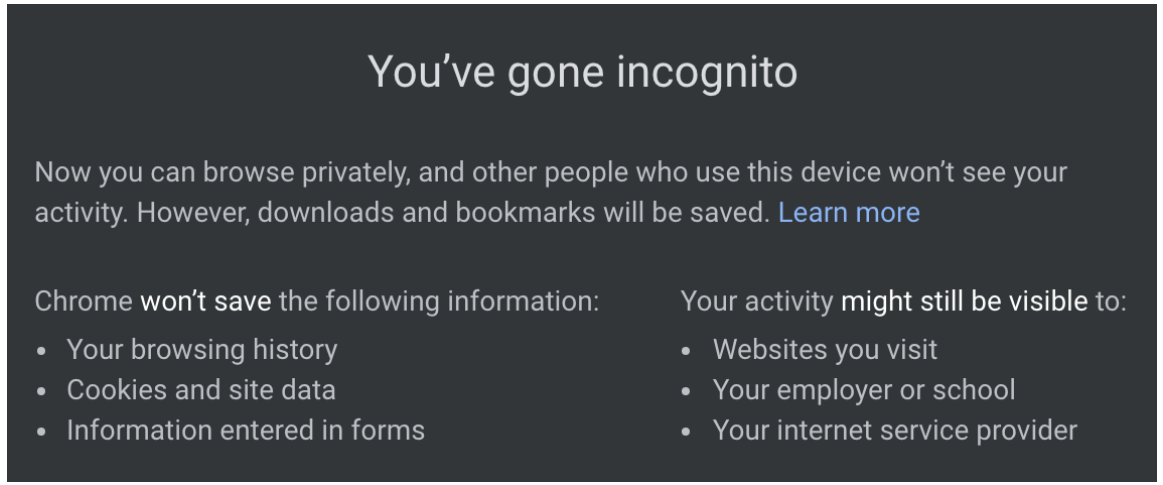
- Do Not Track?

Do Not Track is not a technical defense: trackers must honor the request.

Defenses to Reduce Tracking

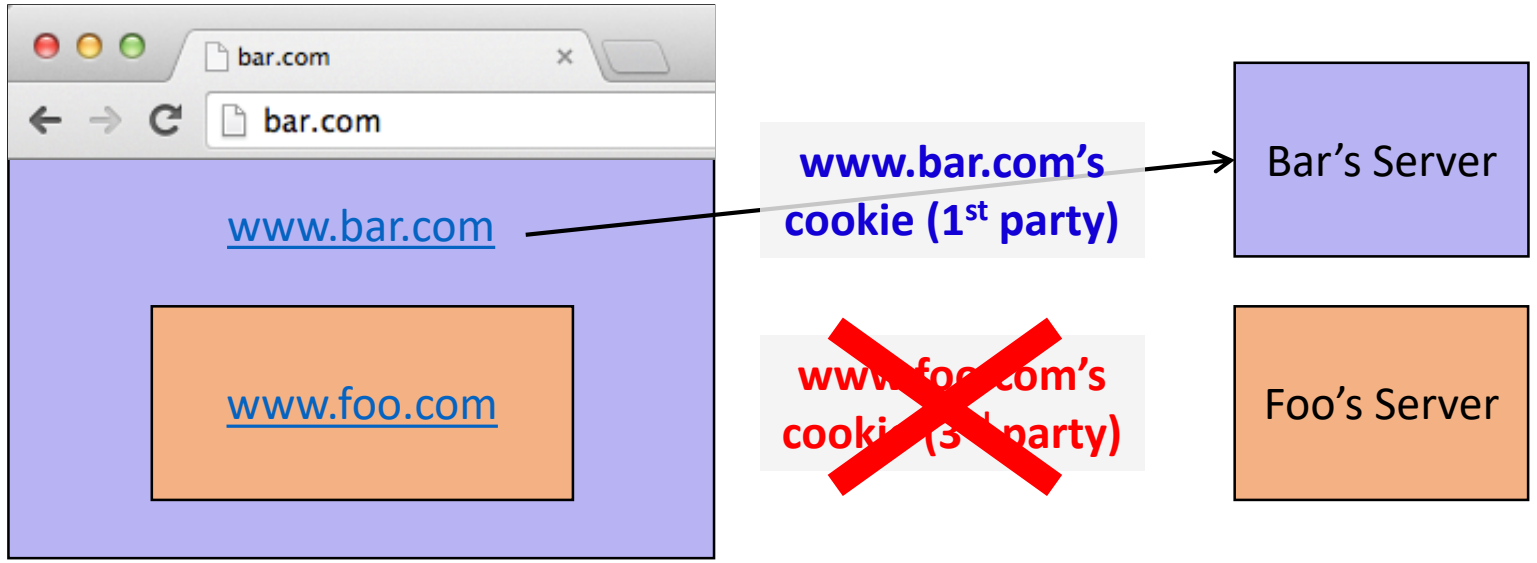
- Do Not Track proposal?
- Private browsing mode?

Private browsing mode doesn't protect against network attackers fully.



Defenses to Reduce Tracking

- Do Not Track proposal?
- Private browsing mode?
- Third-party cookie blocking?



3rd party cookies

- Chrome…

> “By undermining the business model of many ad-supported websites, blunt approaches to cookies encourage the use of opaque techniques such as fingerprinting (an invasive workaround to replace cookies), which can actually reduce user privacy and control. We believe that we as a community can, and must, do better.”
>
> Aug 2022: Remove 3rd party cookies by 2024

The state of 3rd party cookies

- Safari:
  - Blocks most - https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/
- Chrome
  - No longer removing. https://privacysandbox.com/news/privacy-sandbox-next-steps/
- Firefox
  - Specific blocks/etc https://developer.mozilla.org/en-US/blog/goodbye-third-party-cookies/
- Others
  - Variety of behaviors, wide variation

https://www.cookiestatus.com/ -- vaguely up to date (2023)

Cookie ghostwriting

- No 3rd party cookies allowed ☹
- Instead, <script src=https://trackerdomain/cookiewriter.js/>
- No longer in an iframe… what can they do?

Journey to the Center of the Cookie Ecosystem: Unraveling Actors' Roles and Relationships, Sanchez-Rola et al.

Fingerprinting

- An alternative, popular, approach is *fingerprinting*
  - Website runs some javascript to measure browser/machine behavior
  - Generates an ID from this
  - ID is semi-consistent even across things like incognito mode

- Fingerprinting is unaffected by 3rd party cookie changes!