CSE 484: Computer Security and Privacy

Authentication + Tracking

Spring 2024

David Kohlbrenner

dkohlbre@cs

Thanks to Franzi Roesner, Dan Boneh, Dieter Gollmann, Dan Halperin, David Kohlbrenner, Yoshi Kohno, Ada Lerner, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Logistics

- HW3 due Wednesday

- HW2 grades released

- Final project will be covered Monday and released

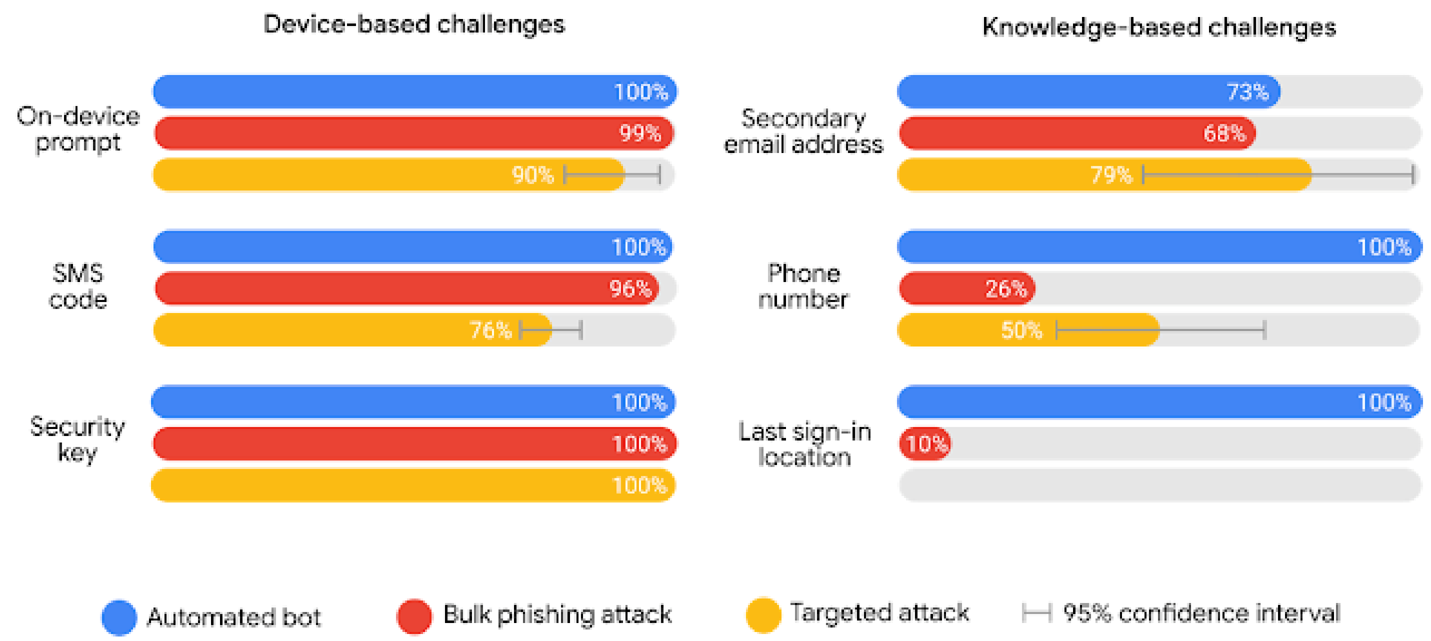
Why does 2FA (sometimes) work?

- Stops phishing, when it is hardware token
- Doesn’t when it is SMS ☹

https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

Secondary Factors Do Help!

Account takeover prevention rates, by challenge type

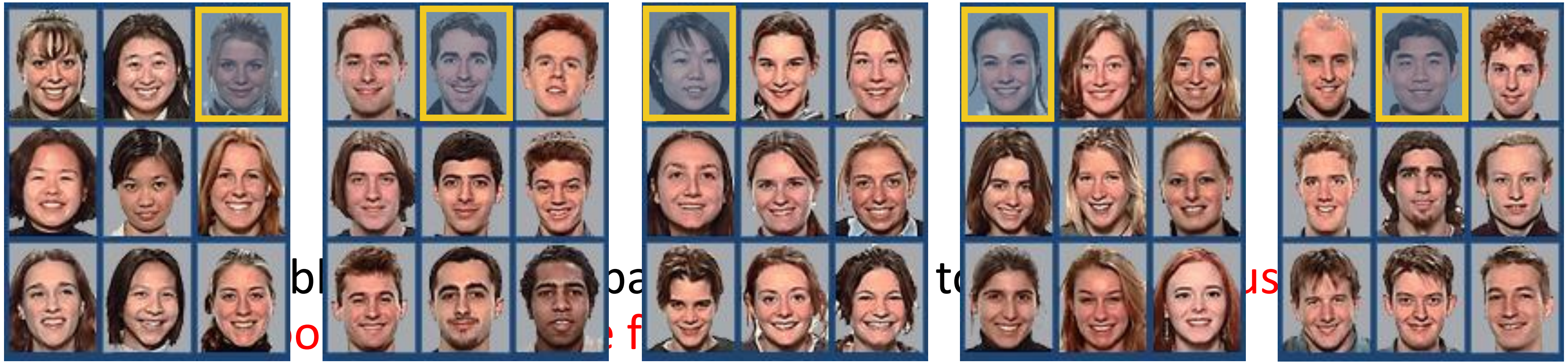


Both device- and knowledge-based challenges help thwart automated bots, while device-based challenges help thwart phishing and even targeted attacks.

Hardware 2FA tokens (U2F/FIDO)

Graphical Passwords

- Many variants… one example: Passfaces
  - Assumption: easy to recall faces

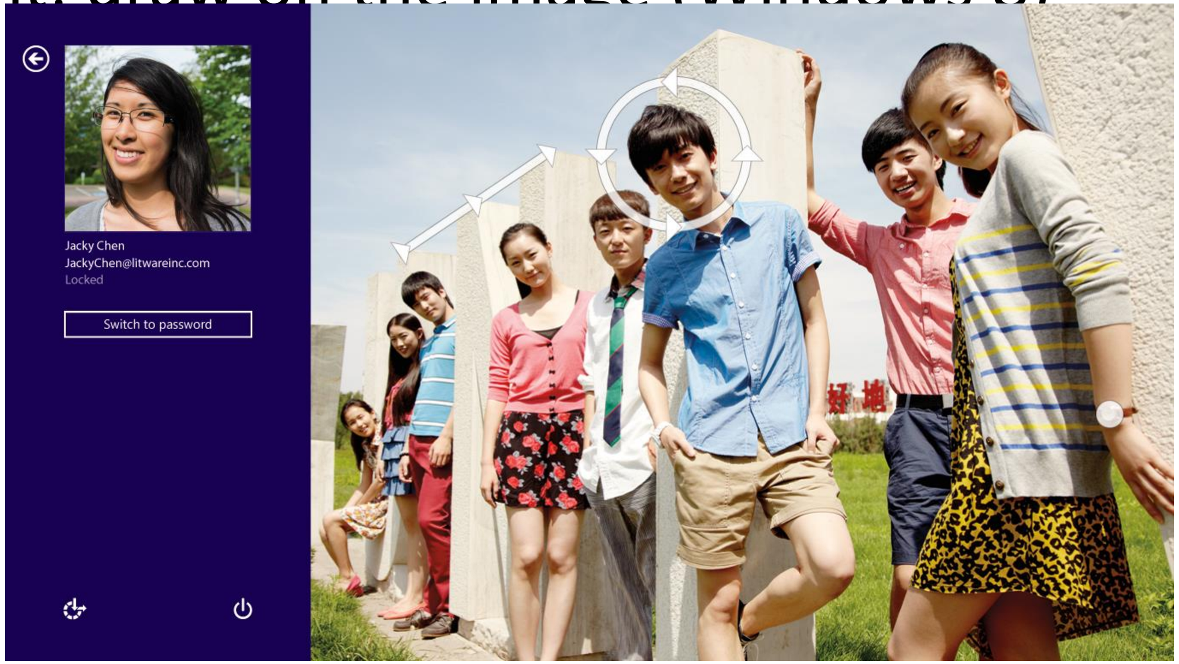


bl pa t us

o e f

Graphical Passwords

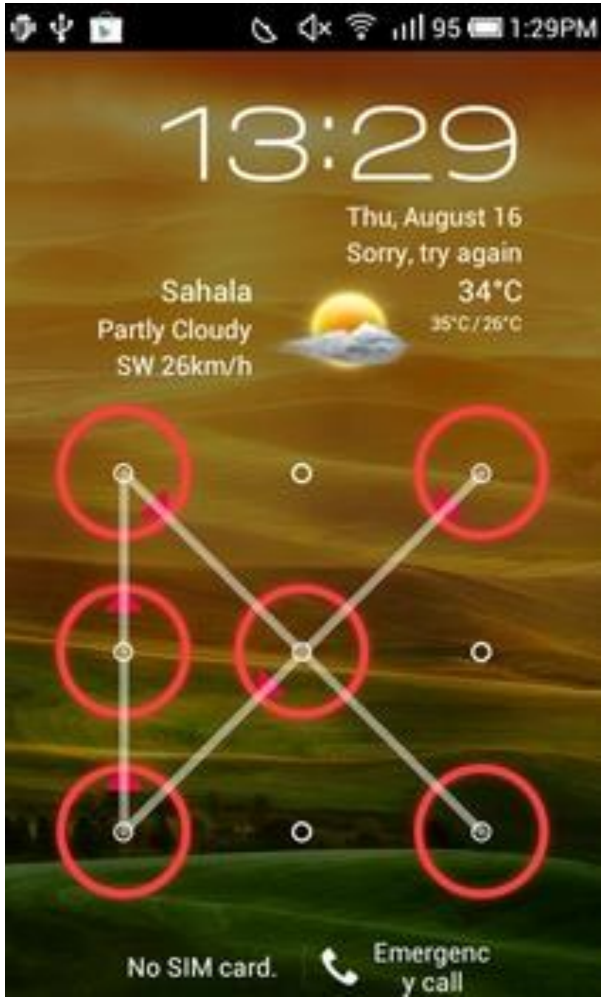
- Another variant: draw on the image (Windows 8)



Jacky Chen
JackyChen@litwareinc.com
Locked

- Problem: users choose predictable points/lines

Unlock Patterns



- Problems:
  - Predictable patterns (familiar pattern by now)
  - Smear patterns
  - Side channels: apps can use accelerometer and gyroscope to extract pattern!

What About Biometrics?

- Authentication: **What you are**
- Unique identifying characteristics to authenticate user or create credentials
  - Biological and physiological: Fingerprints, iris scan
  - Behaviors characteristics - how perform actions: Handwriting, typing, gait
- Advantages:
  - Nothing to remember
  - Passive
  - Can’t share (generally)
  - With perfect accuracy, could be fairly unique

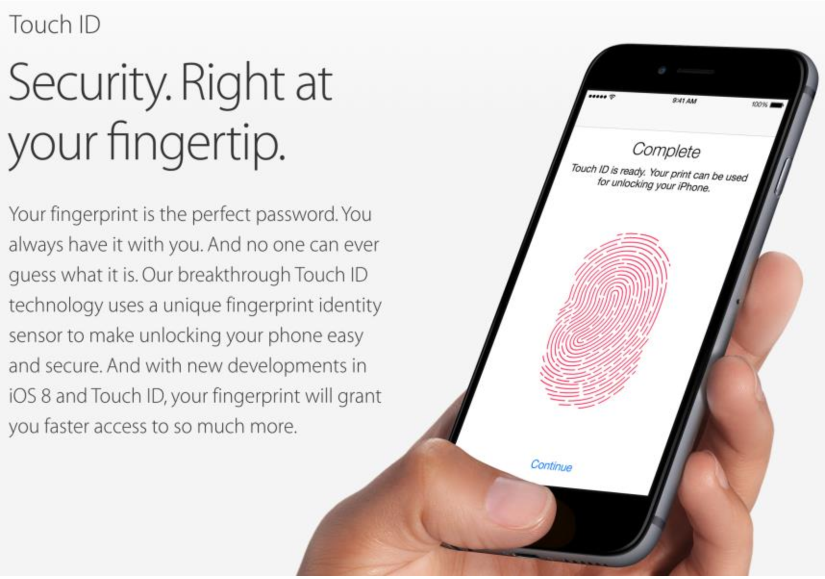
What are reasons to use/*not* use biometrics?

Issues with Biometrics

- Private, but not secret
  - Maybe encoded on the back of an ID card?
  - Maybe encoded on your glass, door handle, ...
  - Sharing between multiple systems?
- Revocation is difficult (impossible?)
  - Sorry, your iris has been compromised, please create a new one...
- Physically identifying
  - Soda machine to cross-reference fingerprint with DMV?
- Birthday paradox
  - With false accept rate of 1 in a million, probability of false match is above 50% with only 1609 samples

Attacking Biometrics

- An adversary might try to steal biometric info
  - Malicious fingerprint reader
    - Consider when biometric is used to derive a cryptographic key
  - Residual fingerprint on a glass



Touch ID

Security. Right at your fingertip.

Your fingerprint is the perfect password. You always have it with you. And no one can ever guess what it is. Our breakthrough Touch ID technology uses a unique fingerprint identity sensor to make unlocking your phone easy and secure. And with new developments in iOS 8 and Touch ID, your fingerprint will grant you faster access to so much more.

9:41 AM
100%
Complete
Touch ID is ready. Your print can be used for unlocking your iPhone.
Continue

Passkeys (2023)

- An actual, deployed, genuine *password replacement*
  - *Also a 2fa replacement!*
  - *And a username replacement!*

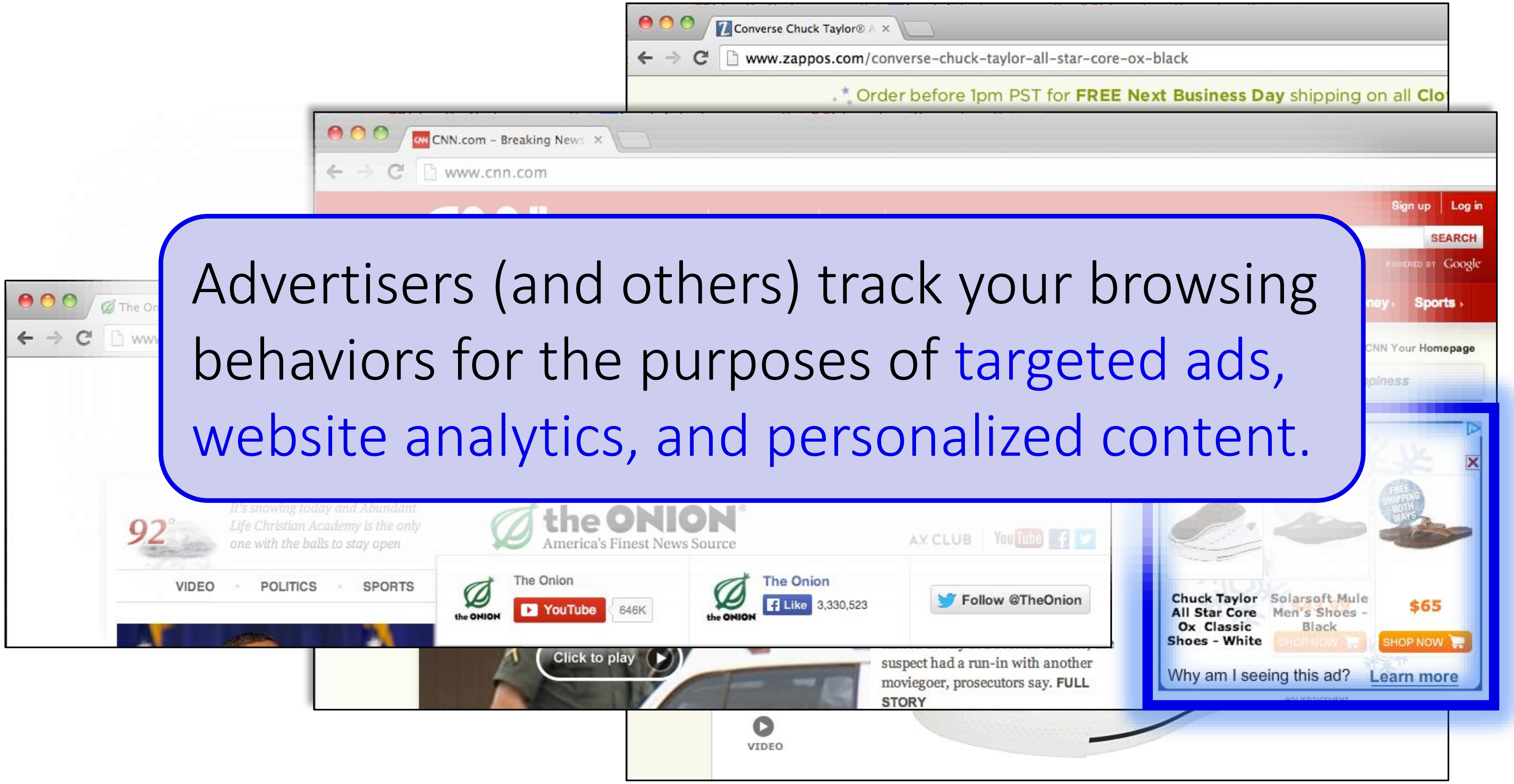
- Basic goals:
  - Store some sort of key on user end-devices
  - Use that key to login to Stuff
  - Don’t allow losing the key
  - Somehow make the key moving between devices Easy

Privacy and web tracking

A topic in flux

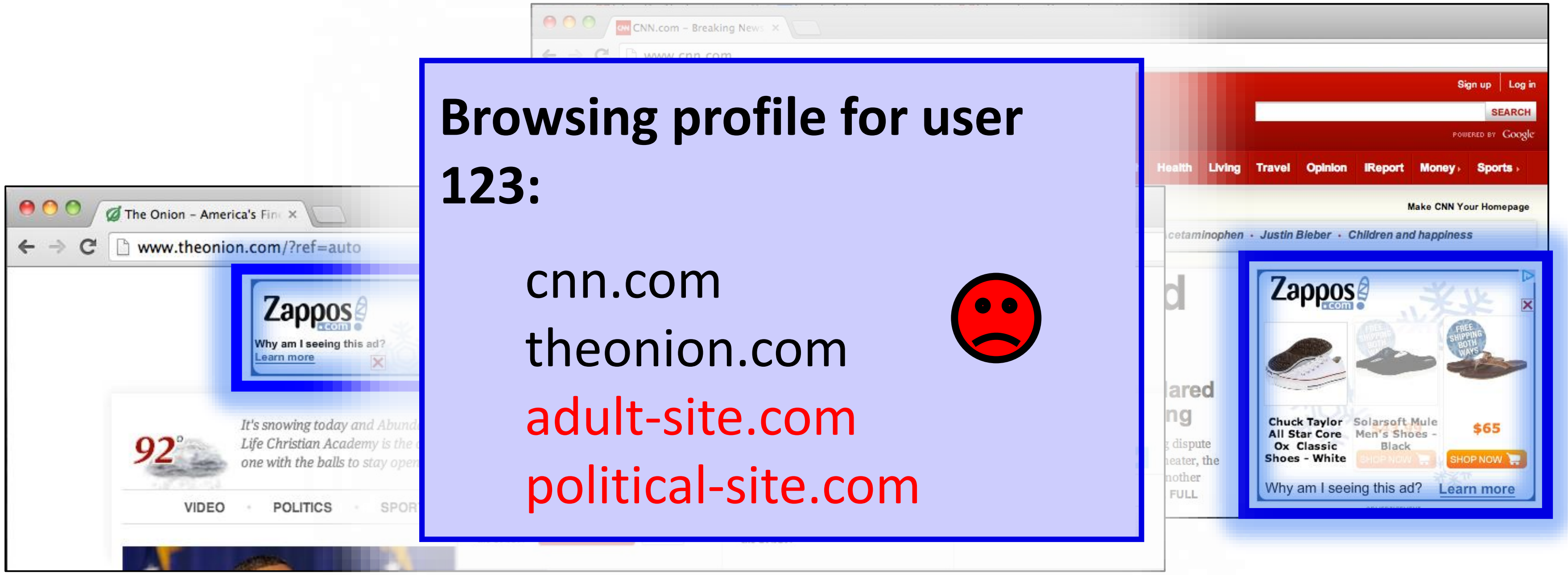
- Tracking via cookies
- Tracking via other methods
- Fingerprinting

Ads That Follow You


Converse Chuck Taylor®
www.zappos.com/converse-chuck-taylor-all-star-core-ox-black
Order before 1pm PST for FREE Next Business Day shipping on all Clo
CNN.com – Breaking News
www.cnn.com
Sign up
Log in
SEARCH
POWERED BY Google
Sports
CNN Your Homepage
The Onion
92°
It's snowing today and Abundant Life Christian Academy is the only one with the balls to stay open
the ONION America's Finest News Source
A.V. CLUB
VIDEO
POLITICS
SPORTS
The Onion
YouTube
646K
Like
3,330,523
Follow @TheOnion
Click to play
suspect had a run-in with another moviegoer, prosecutors say. FULL STORY
VIDEO
FREE SHIPPING BOTH WAYS
Chuck Taylor All Star Core Ox Classic Shoes - White
Solarsoft Mule Men's Shoes - Black
$65
SHOP NOW
Why am I seeing this ad?
Learn more

Advertisers (and others) track your browsing behaviors for the purposes of targeted ads, website analytics, and personalized content.

Third-Party Web Tracking



Browsing profile for user 123:

cnn.com
theonion.com
adult-site.com
political-site.com

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

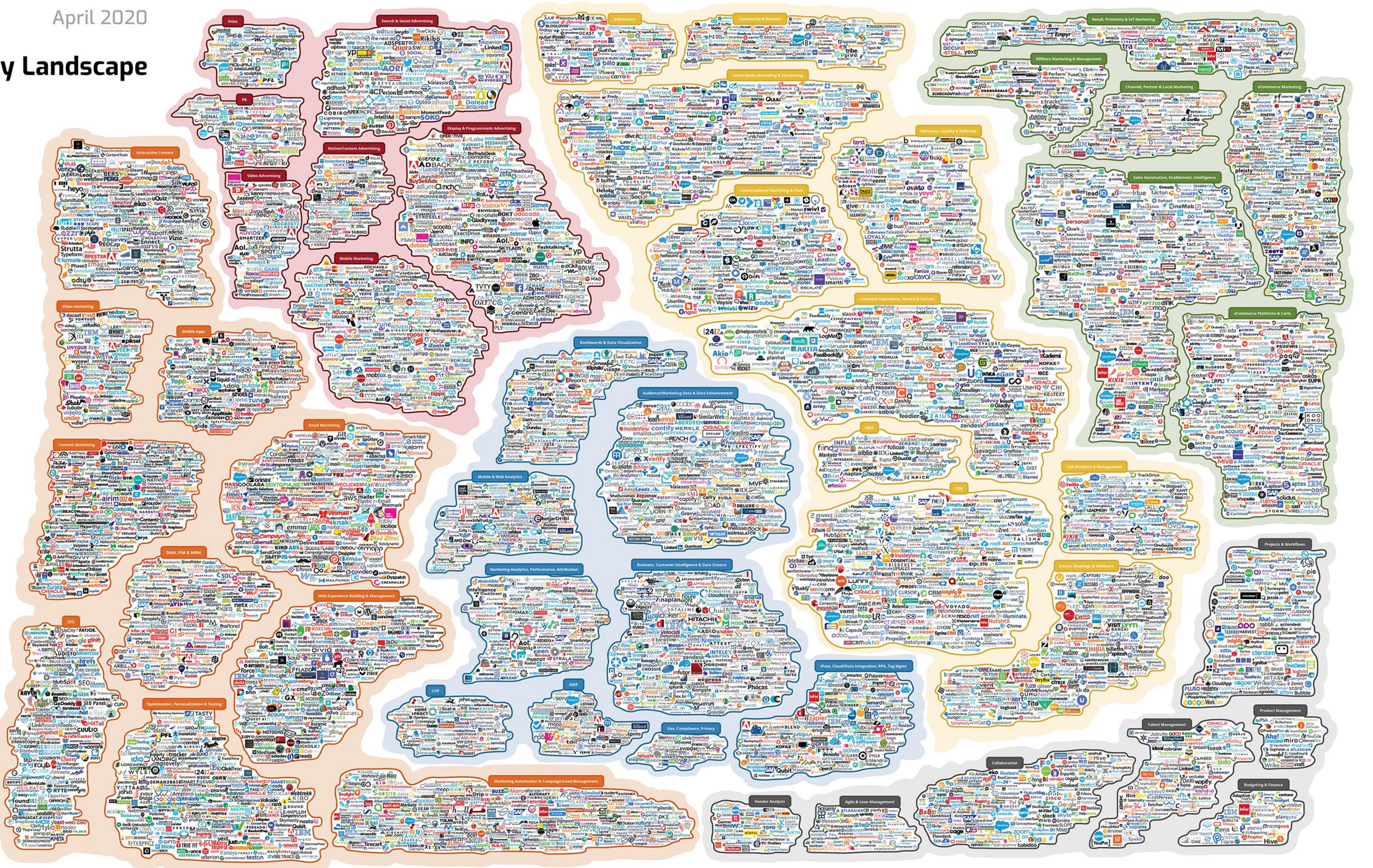
Marketing Technology Landscape

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

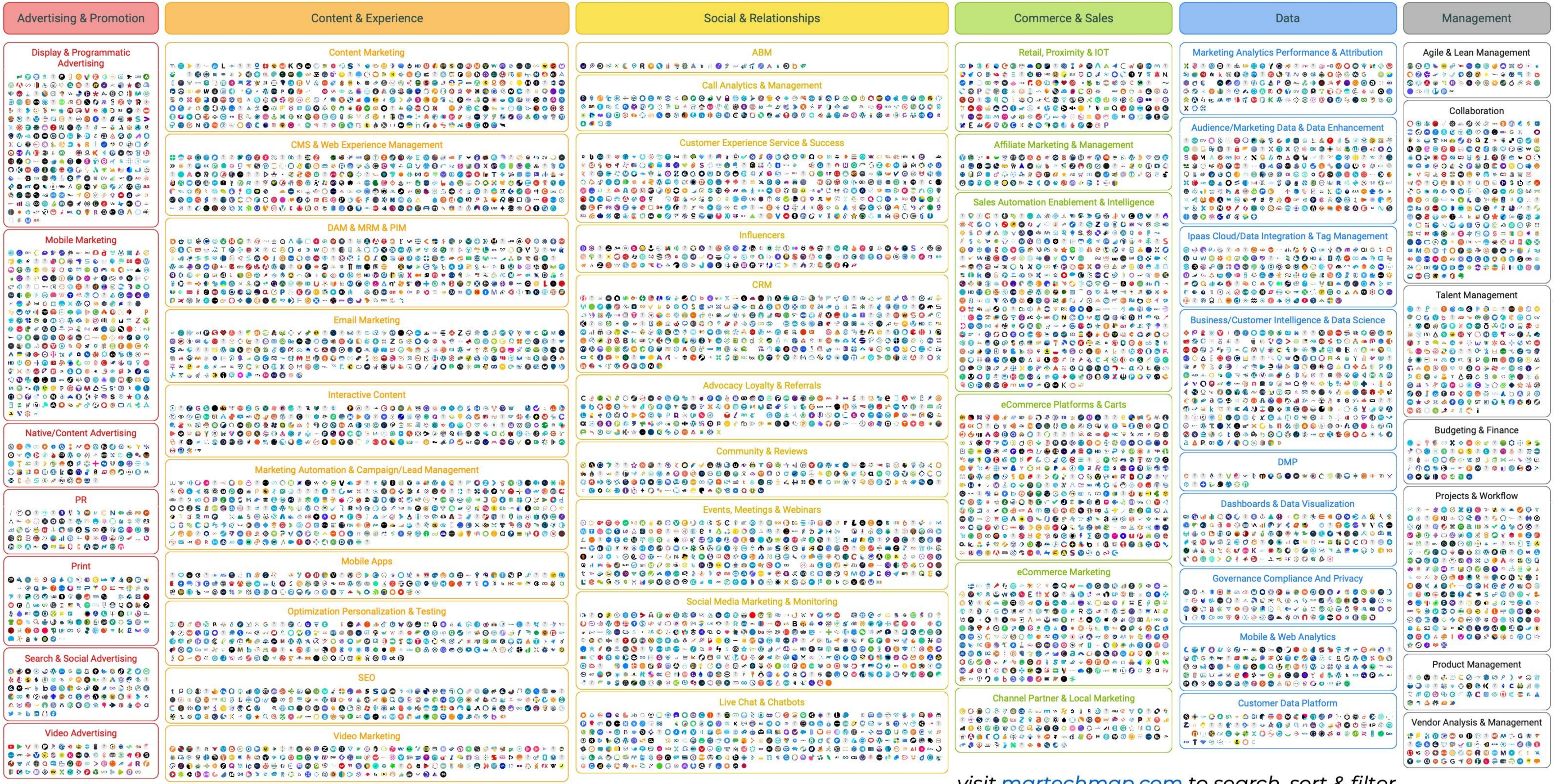
2019	7,040 solutions
2018	6,829 solutions
2017	5,381 solutions
2016	3,874 solutions
2015	1,876 solutions
2014	947 solutions


Print
Search & Social Advertising
PR
Display & Programmatic Advertising
Native/Content Advertising
Video Advertising
Mobile Marketing
Interactive Content
Video Marketing
Mobile Apps
Email Marketing
Content Marketing
DAM, PIM & MRM
Web Experience Building & Management
SEO
Optimization, Personalization & Testing
Marketing Automation & Campaign/Lead Management
Influencers
Community & Reviews
Social Media Marketing & Monitoring
Advocacy, Loyalty & Referrals
Conversational Marketing & Chat
Customer Experience, Service & Success
ABM
Call Analytics & Management
CRM
Events, Meetings & Webinars
Retail, Proximity & IoT Marketing
Affiliate Marketing & Management
Channel, Partner & Local Marketing
eCommerce Marketing
Sales Automation, Enablement, Intelligence
eCommerce Platforms & Carts
Dashboards & Data Visualization
Audience/Marketing Data & Data Enhancement
Mobile & Web Analytics
Marketing Analytics, Performance, Attribution
Business/Customer Intelligence & Data Science
CDP
DMP
Gov, Compliance, Privacy
iPaaS, Cloud/Data Integration, RPA, Tag Mgmt
Projects & Workflows
Product Management
Talent Management
Collaboration
Budgeting & Finance
Vendor Analysis
Agile & Lean Management

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

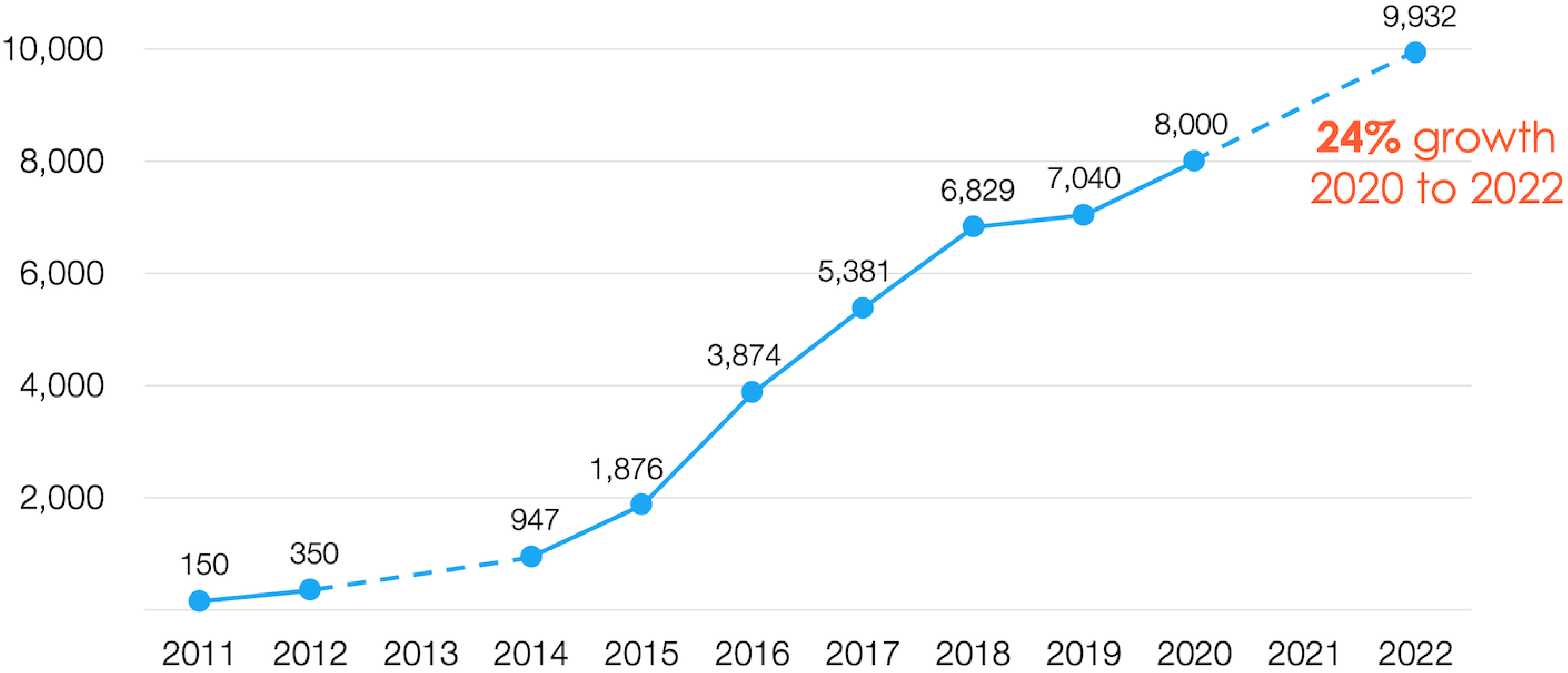
- Marketing Analytics Performance & Attribution
- Audience/Marketing Data & Data Enhancement
- Ipaas Cloud/Data Integration & Tag Management
- Business/Customer Intelligence & Data Science
- DMP
- Dashboards & Data Visualization
- Governance Compliance And Privacy
- Mobile & Web Analytics
- Customer 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

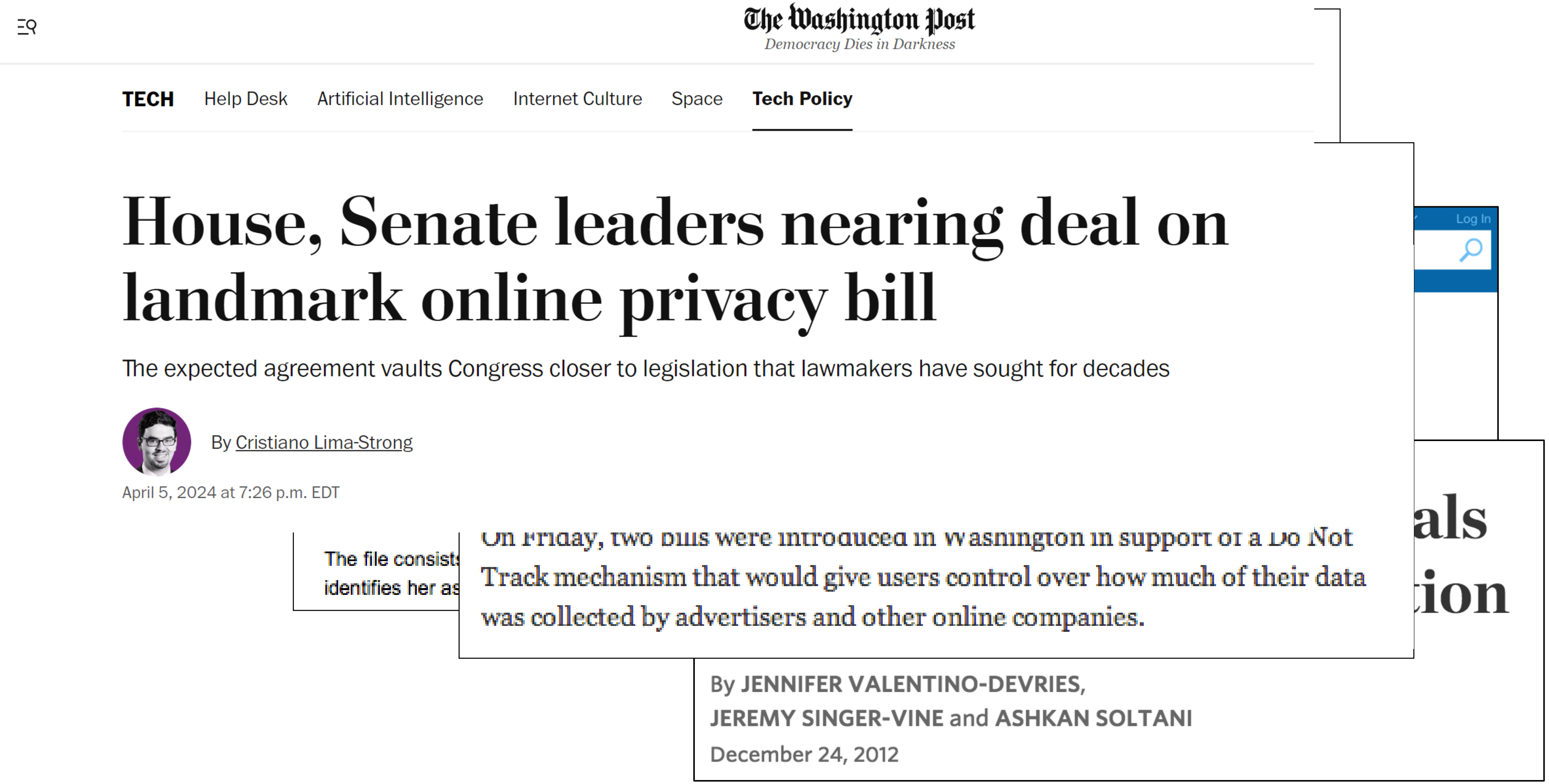
6,521% growth 2011 to 2022



24% growth 2020 to 2022

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

Concerns About Privacy



The Washington Post
Democracy Dies in Darkness

House, Senate leaders nearing deal on landmark online privacy bill

The expected agreement vaults Congress closer to legislation that lawmakers have sought for decades

By Cristiano Lima-Strong

April 5, 2024 at 7:26 p.m. EDT

The file consist
identifies her as

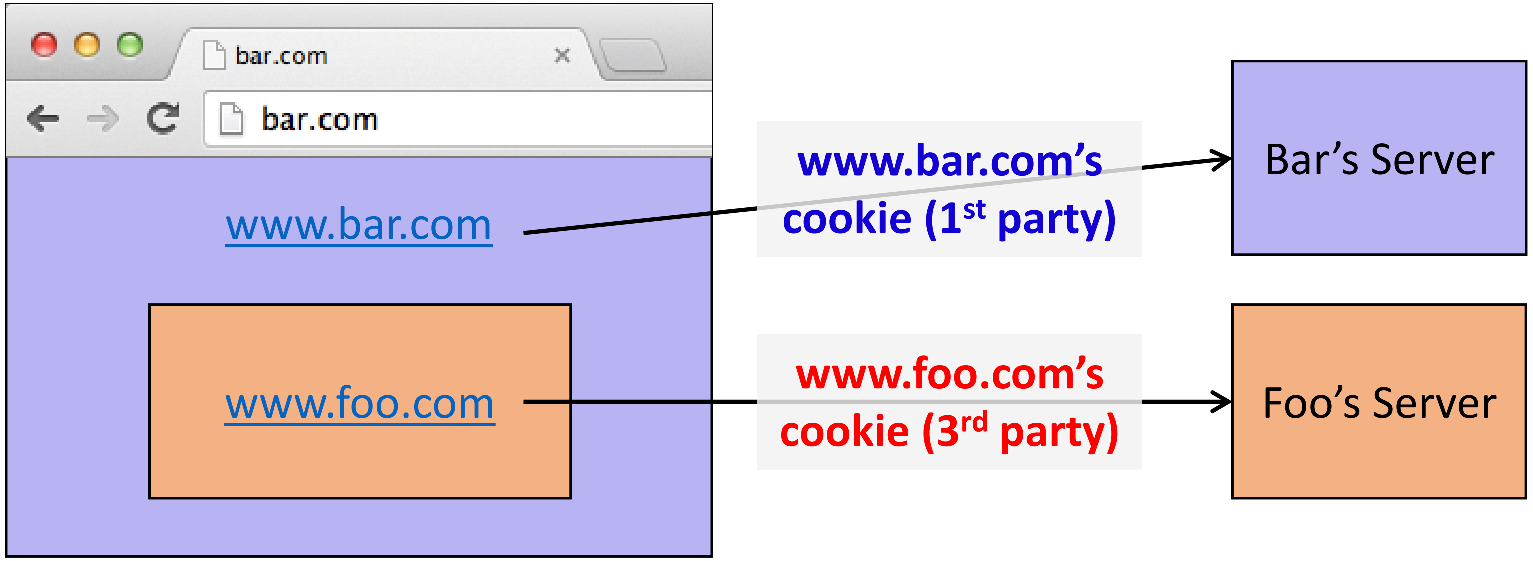
On Friday, two bills were introduced in Washington in support of a Do Not Track mechanism that would give users control over how much of their data was collected by advertisers and other online companies.

als
ion

By JENNIFER VALENTINO-DEVRIES,
JEREMY SINGER-VINE and ASHKAN SOLTANI
December 24, 2012

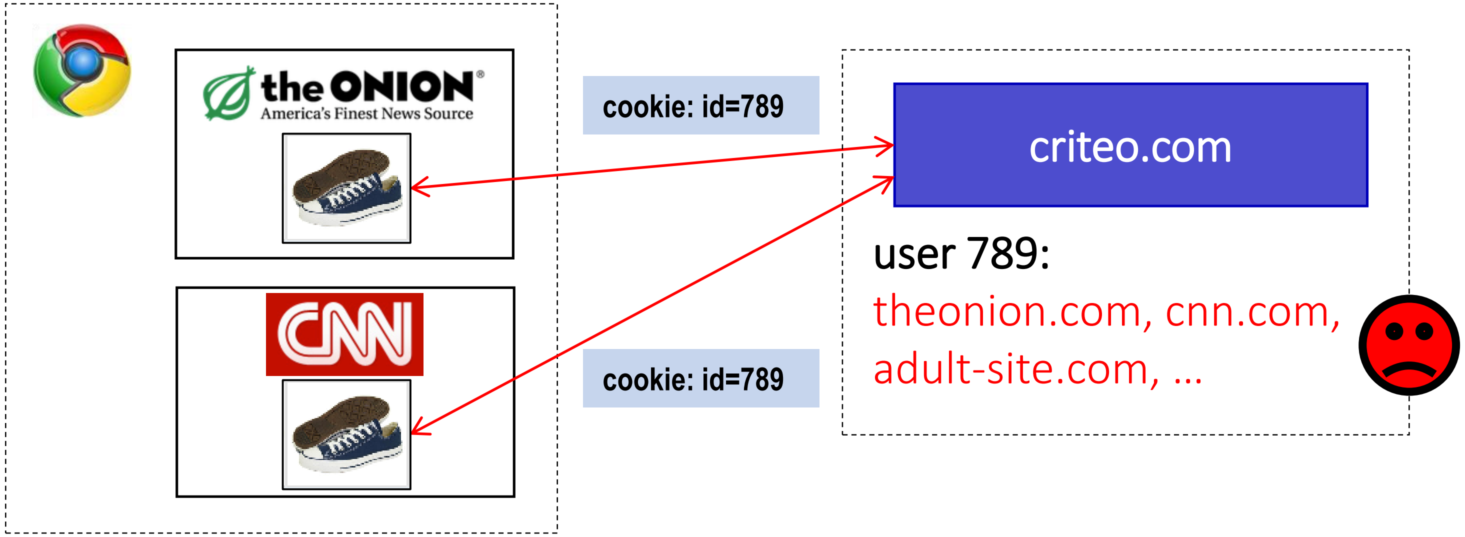
First and Third Parties

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


bar.com
bar.com
www.bar.com
www.foo.com
www.bar.com's cookie (1st party)
www.foo.com's cookie (3rd party)
Bar's Server
Foo's Server

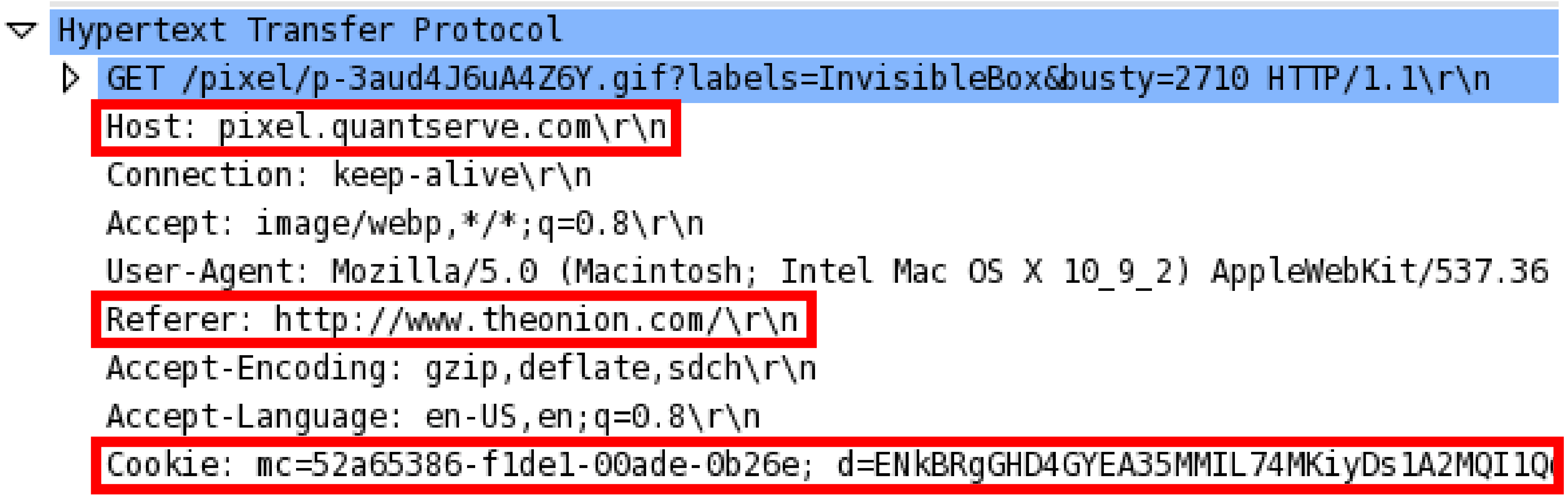
Anonymous Tracking

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.



```
Hypertext Transfer Protocol
  GET /pixel/p-3aud4J6uA4Z6Y.gif?labels=InvisibleBox&busty=2710 HTTP/1.1\r\n
  Host: pixel.quantserve.com\r\n
  Connection: keep-alive\r\n
  Accept: image/webp,*/*;q=0.8\r\n
  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_2) AppleWebKit/537.36
  Referer: http://www.theonion.com/\r\n
  Accept-Encoding: gzip,deflate,sdch\r\n
  Accept-Language: en-US,en;q=0.8\r\n
  Cookie: mc=52a65386-f1de1-00ade-0b26e; d=ENkBRgGHD4GYEA35MMIL74MKiyDs1A2MQI1Q
```

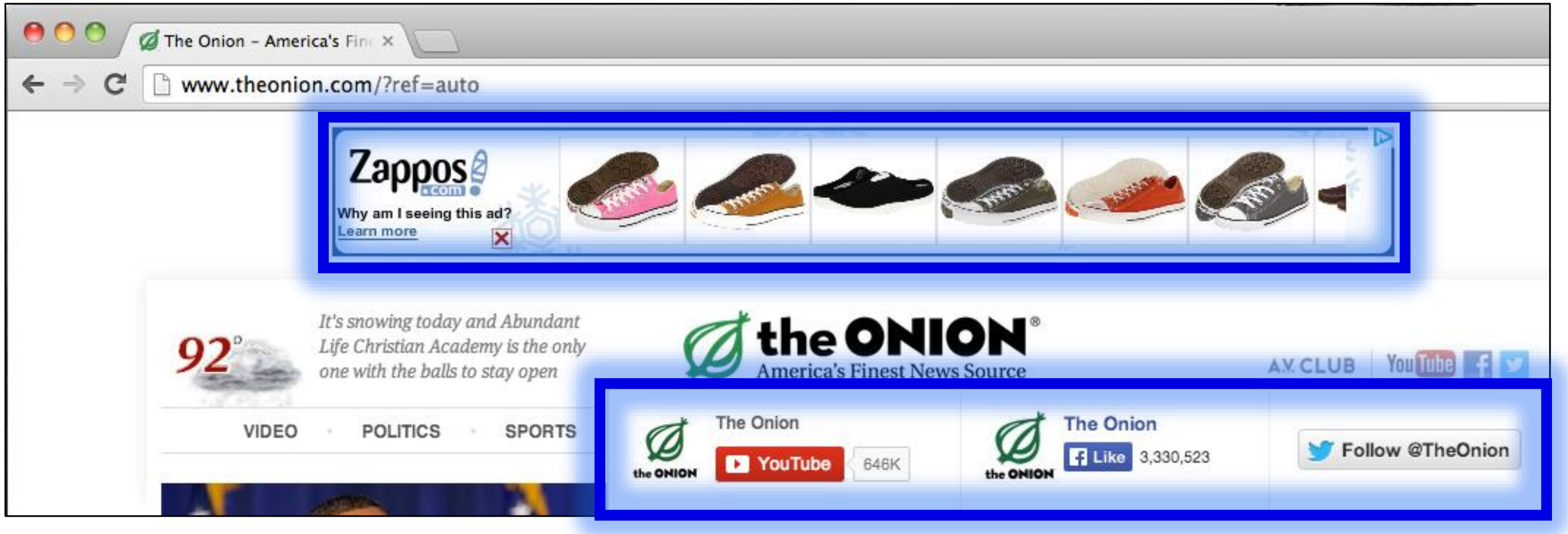
Tracking Technologies

- 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

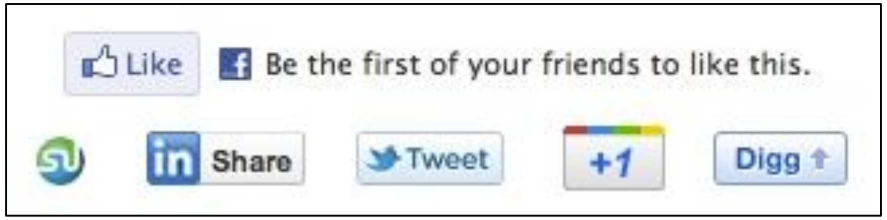
- "Zombie" cookies that respawn (http://samy.pl/evercookie)

Other Trackers?



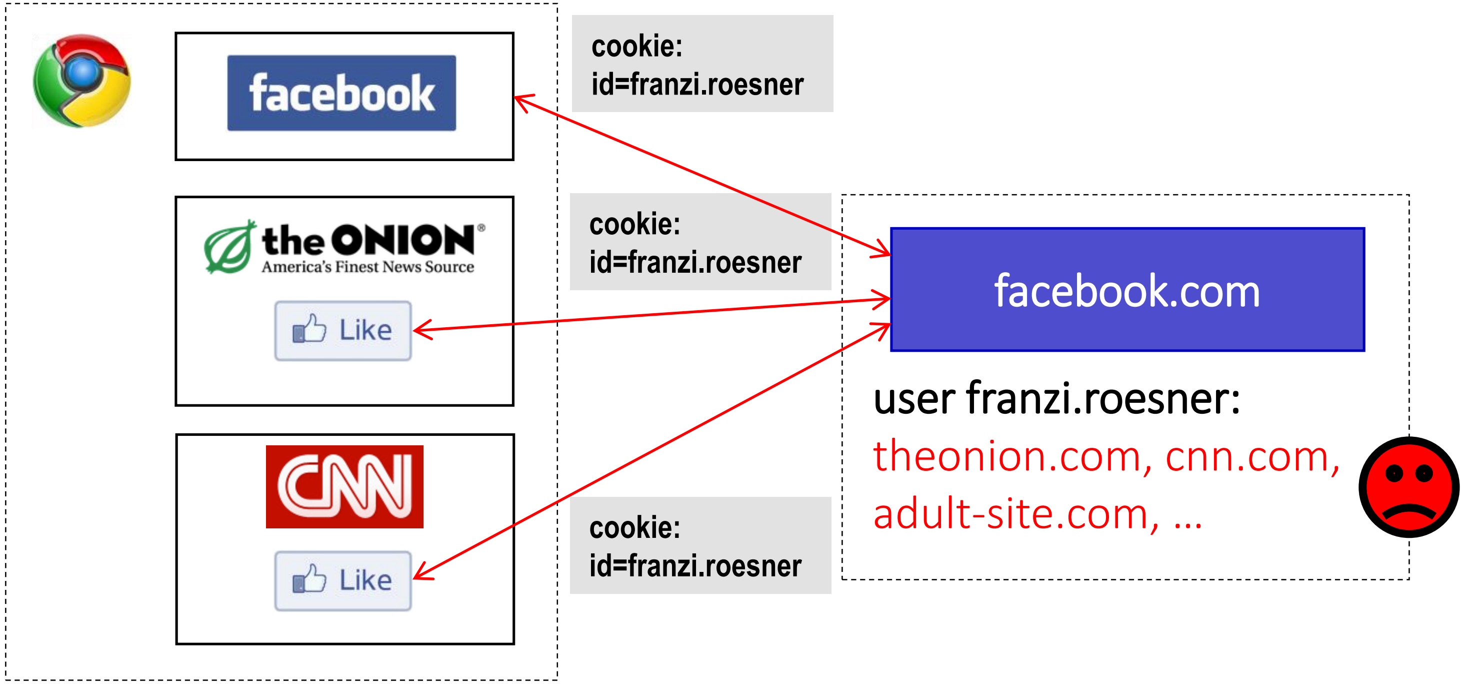
It's snowing today and Abundant Life Christian Academy is the only one with the balls to stay open

“Personal” Trackers



Be the first of your friends to like this.

Personal Tracking


facebook
the ONION America's Finest News Source
Like
CNN
Like
cookie: id=franzi.roesner
cookie: id=franzi.roesner
cookie: id=franzi.roesner
facebook.com
user franzi.roesner:
theonion.com, cnn.com, adult-site.com, …

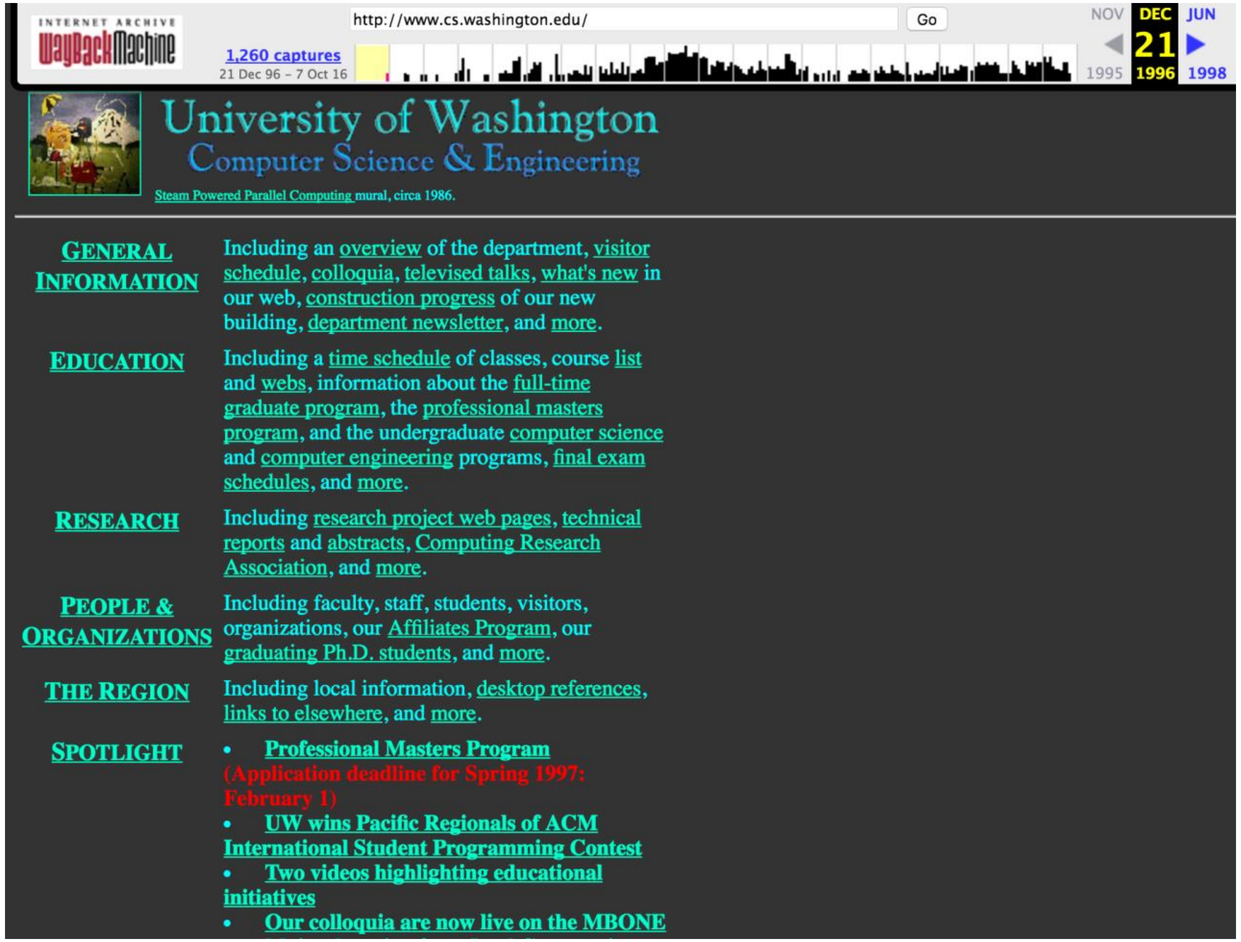
- Tracking is not anonymous (linked to accounts).
- Users directly visit tracker's site → evades some defenses.

How has this changed over time?

- The web has existed for a while now…
  - What about tracking before 2011?
  - What about tracking before 2009?

- Solution: time travel!

The Wayback Machine to the Rescue



University of Washington
Computer Science & Engineering

Steam Powered Parallel Computing mural, circa 1986.

GENERAL INFORMATION Including an overview of the department, visitor schedule, colloquia, televised talks, what's new in our web, construction progress of our new building, department newsletter, and more.

EDUCATION Including a time schedule of classes, course list and webs, information about the full-time graduate program, the professional masters program, and the undergraduate computer science and computer engineering programs, final exam schedules, and more.

RESEARCH Including research project web pages, technical reports and abstracts, Computing Research Association, and more.

PEOPLE & ORGANIZATIONS Including faculty, staff, students, visitors, organizations, our Affiliates Program, our graduating Ph.D. students, and more.

THE REGION Including local information, desktop references, links to elsewhere, and more.

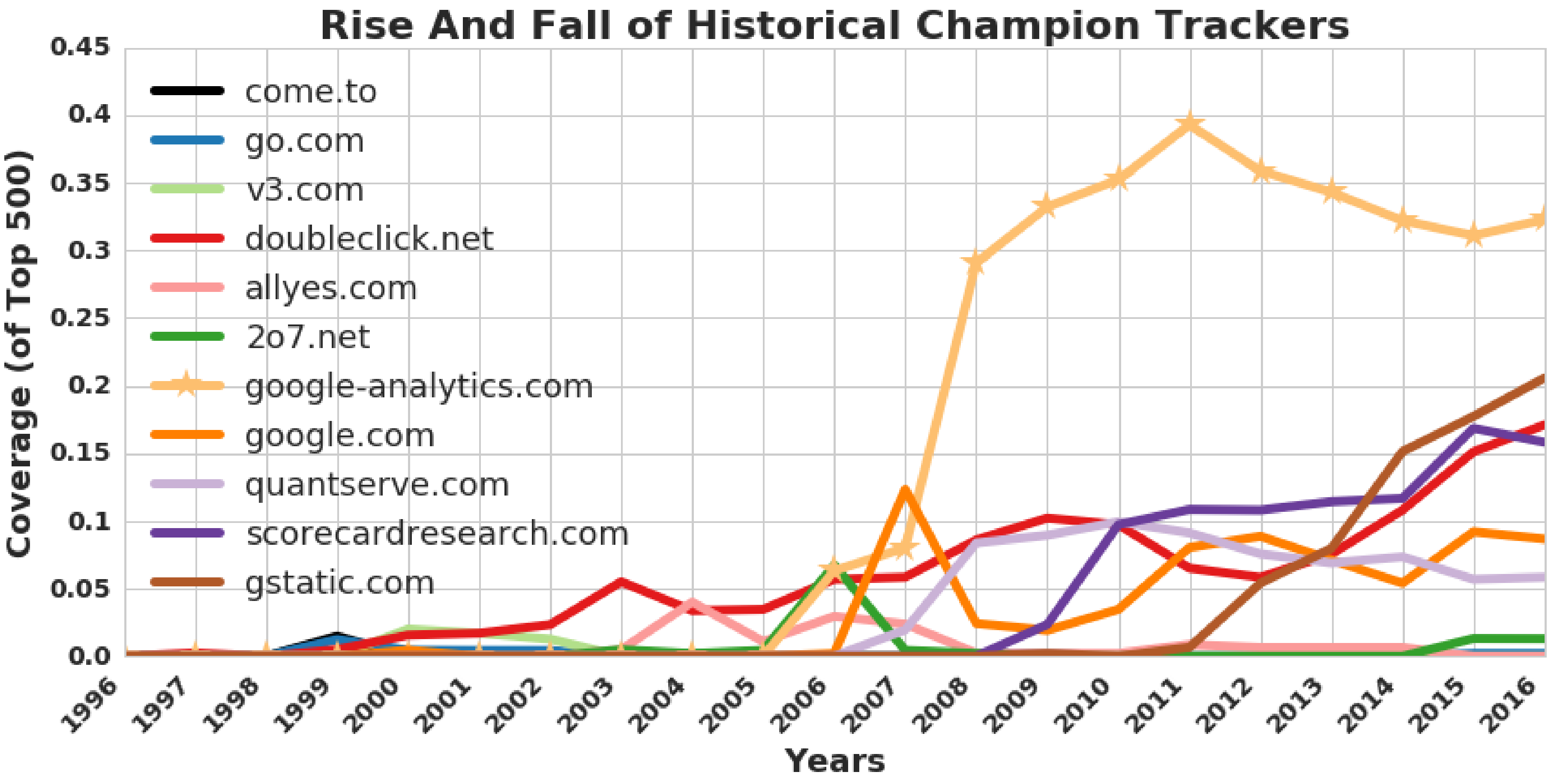
SPOTLIGHT

- **Professional Masters Program** (Application deadline for Spring 1997: February 1)
- **UW wins Pacific Regionals of ACM International Student Programming Contest**
- **Two videos highlighting educational initiatives**
- **Our colloquia are now live on the MBONE**

Time travel for web tracking: http://trackingexcavator.cs.washington.edu

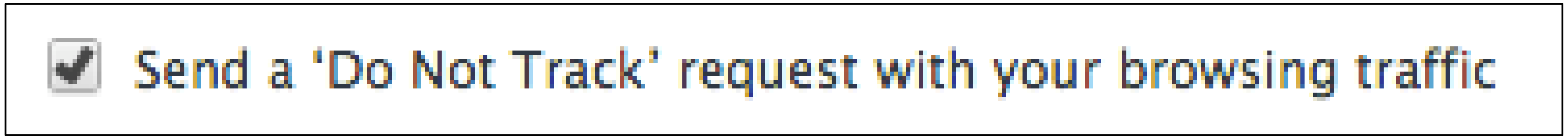
1996-2016: More & More Tracking

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



Defenses to Reduce Tracking

- Do Not Track?



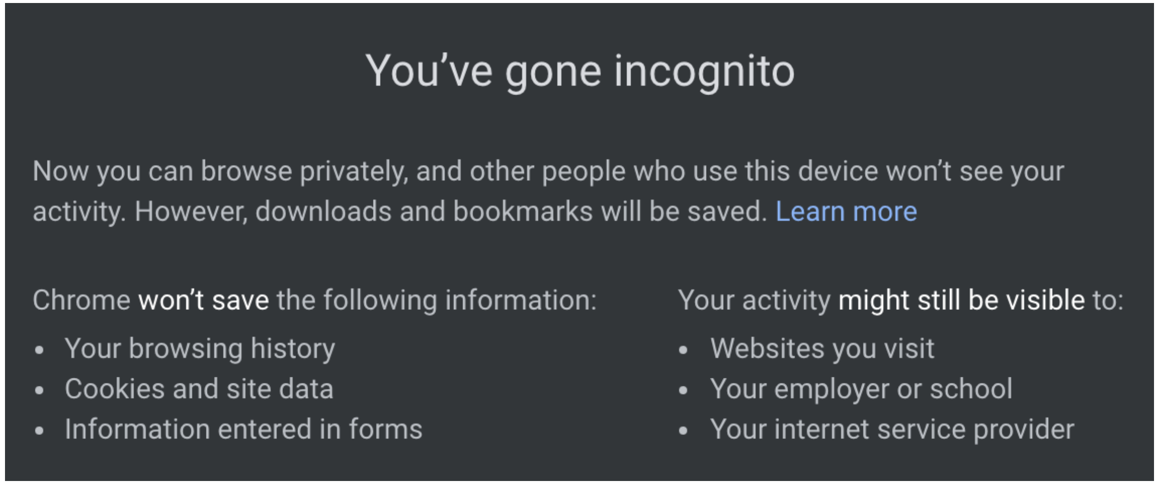
☑ Send a 'Do Not Track' request with your browsing traffic

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.



You've gone incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. Learn more

Chrome **won't save** the following information:

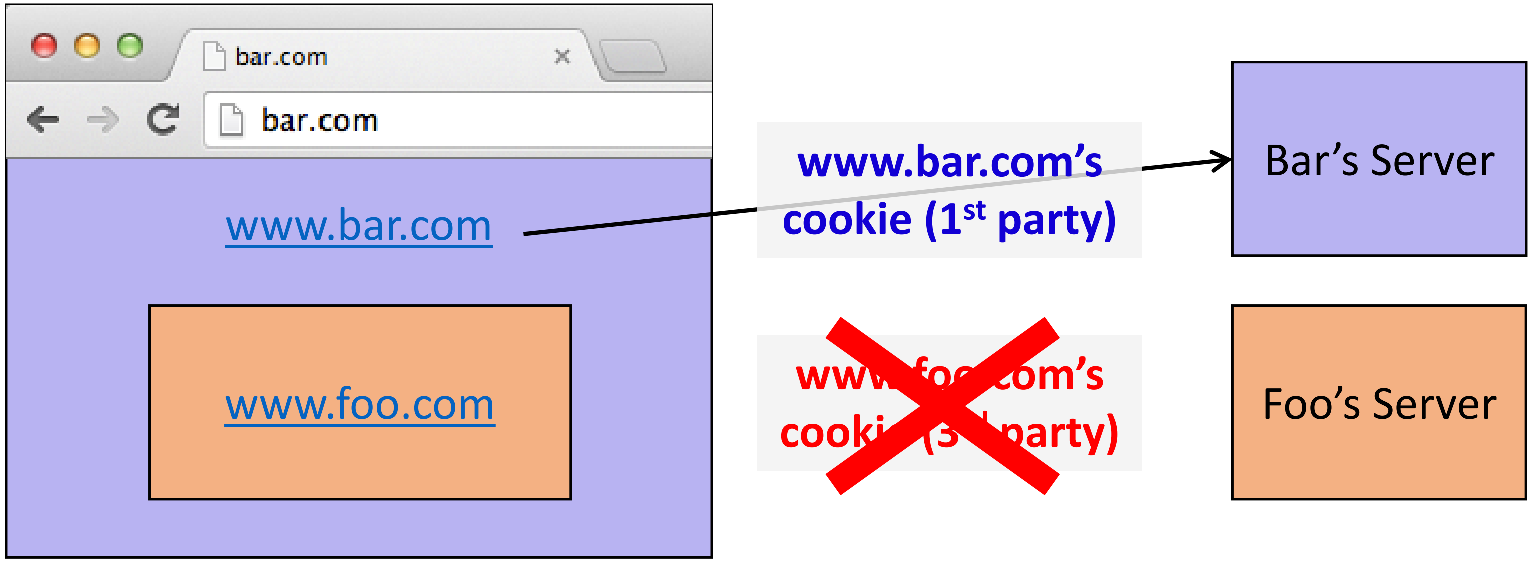
- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity **might still be visible** to:

- Websites you visit
- Your employer or school
- Your internet service provider

Defenses to Reduce Tracking

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


bar.com
bar.com
www.bar.com
www.foo.com
www.bar.com's cookie (1st party)
~~www.foo.com's cookie (3rd party)~~
Bar's Server
Foo's Server

3rd party cookies

- Safari and FF (mostly) now block 3rd party cookies
  - https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/
  - https://blog.mozilla.org/blog/2019/09/03/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/

- 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