

CSE 484: Computer Security and Privacy

Web Security

[Web Privacy]

Winter 2021

David Kohlbrenner

dkohlbre@cs.washington.edu

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

...

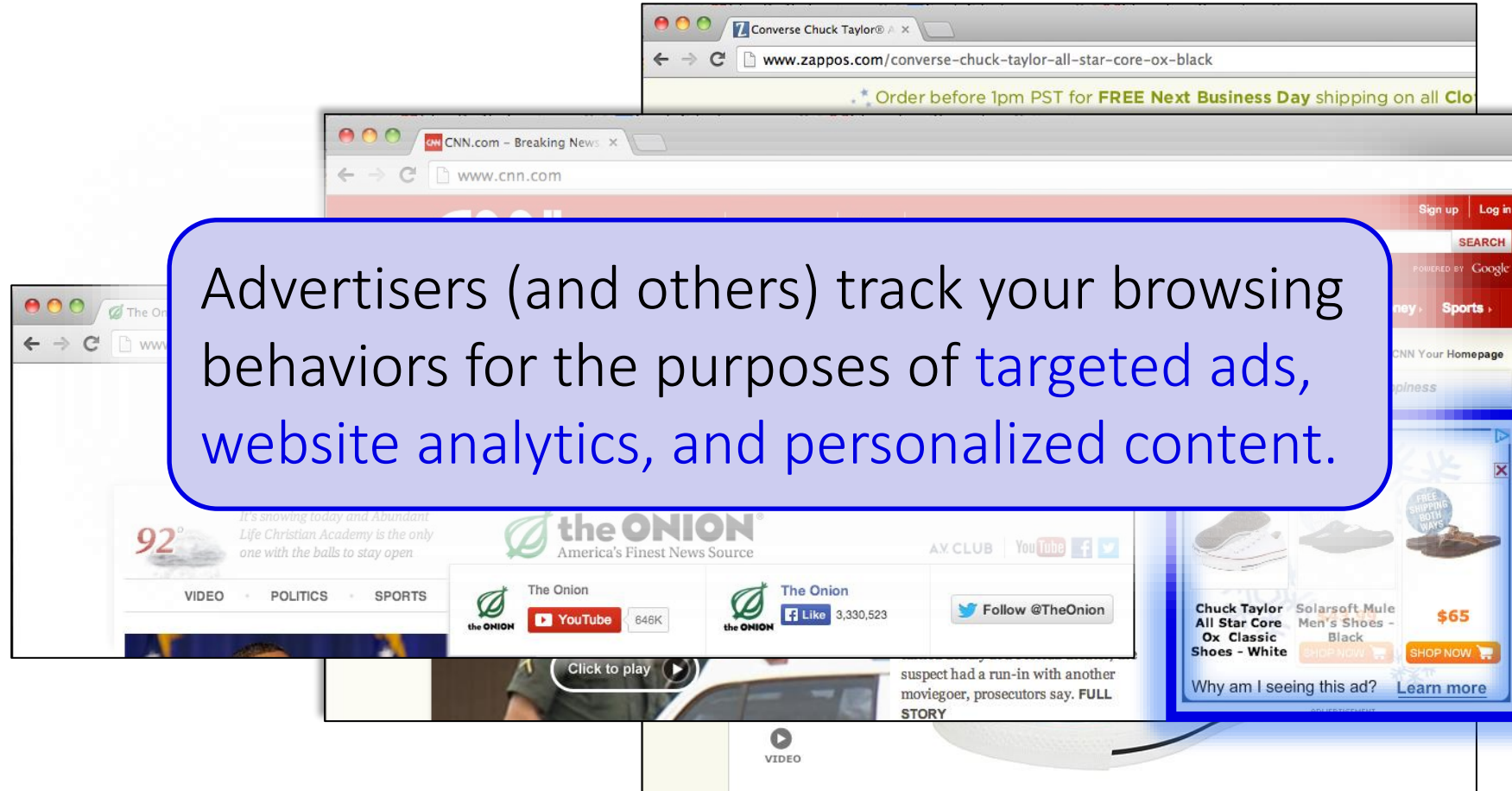
Admin

- Lab 2:
 - Check access ASAP
 - Read FAQs 😊
- Homework 3: out soon, due 03/5
- Guest lecture on Wednesday
 - Alex Gantman – Qualcomm – Embedded systems security and careers

A topic in flux

- Tracking via cookies
- Tracking via other methods
- Fingerprinting


Ads That Follow You



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.

Concerns About Privacy

THE WALL STREET JOURNAL.
WHAT THEY KNOW | JULY 30, 2010

The New York Times
May 6, 2011, 5:01 pm | 3 Comments

'Do Not Track' Privacy Bill Appears in Congress

By TANZINA VEGA

And the privacy legislation just keeps on coming.

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.

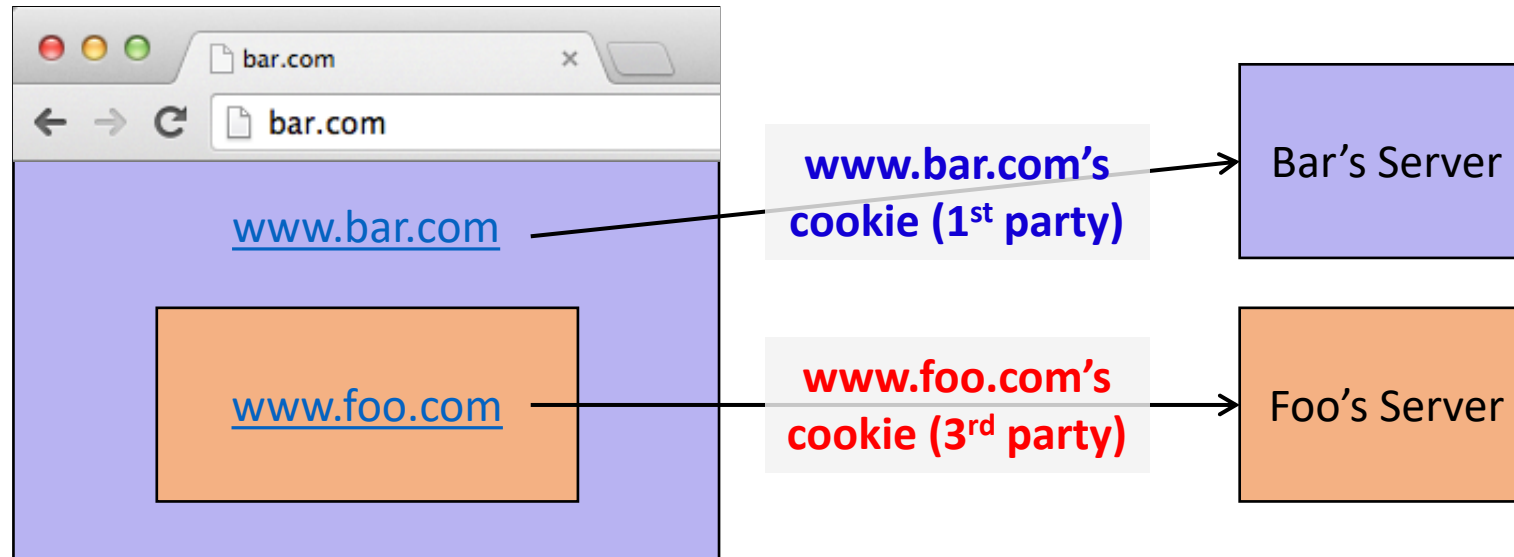
By JENNIFER VALENTINO-DEVRIES,
JEREMY SINGER-VINE and ASHKAN SOLTANI
December 24, 2012

Log In

als
ion

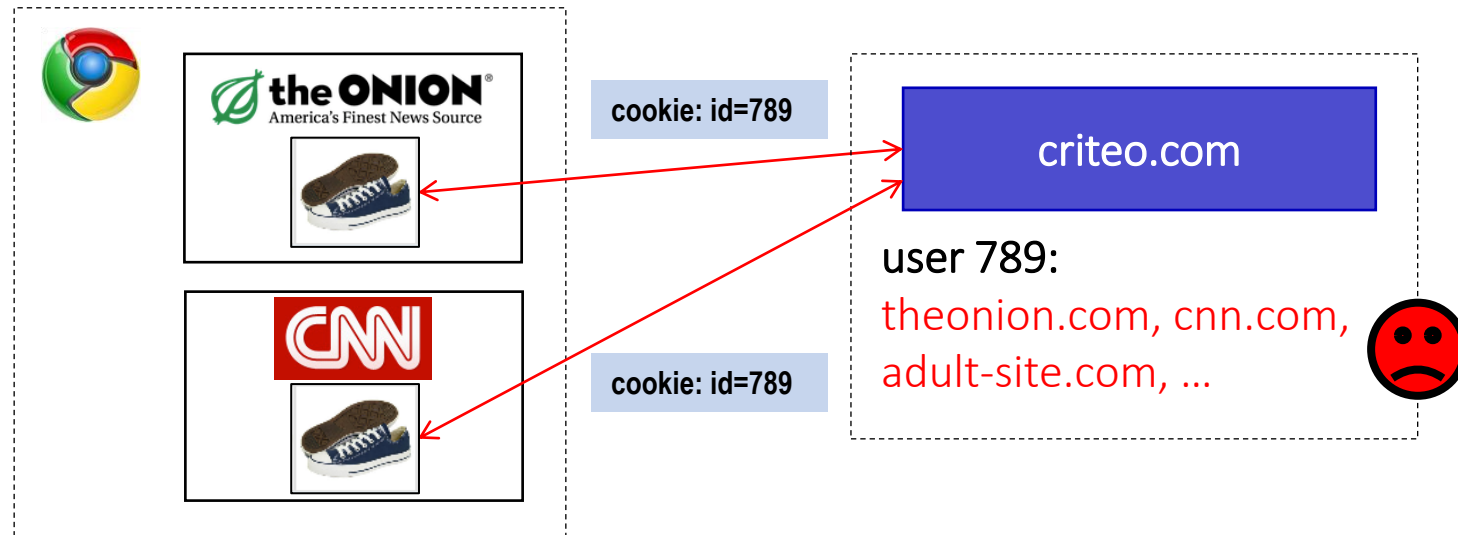
First and Third Parties

- **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.

▼ Hypertext Transfer Protocol

▶ GET /pixel/p-3aud4J6uA4Z6Y.gif?labels=InvisibleBox&bust=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>)

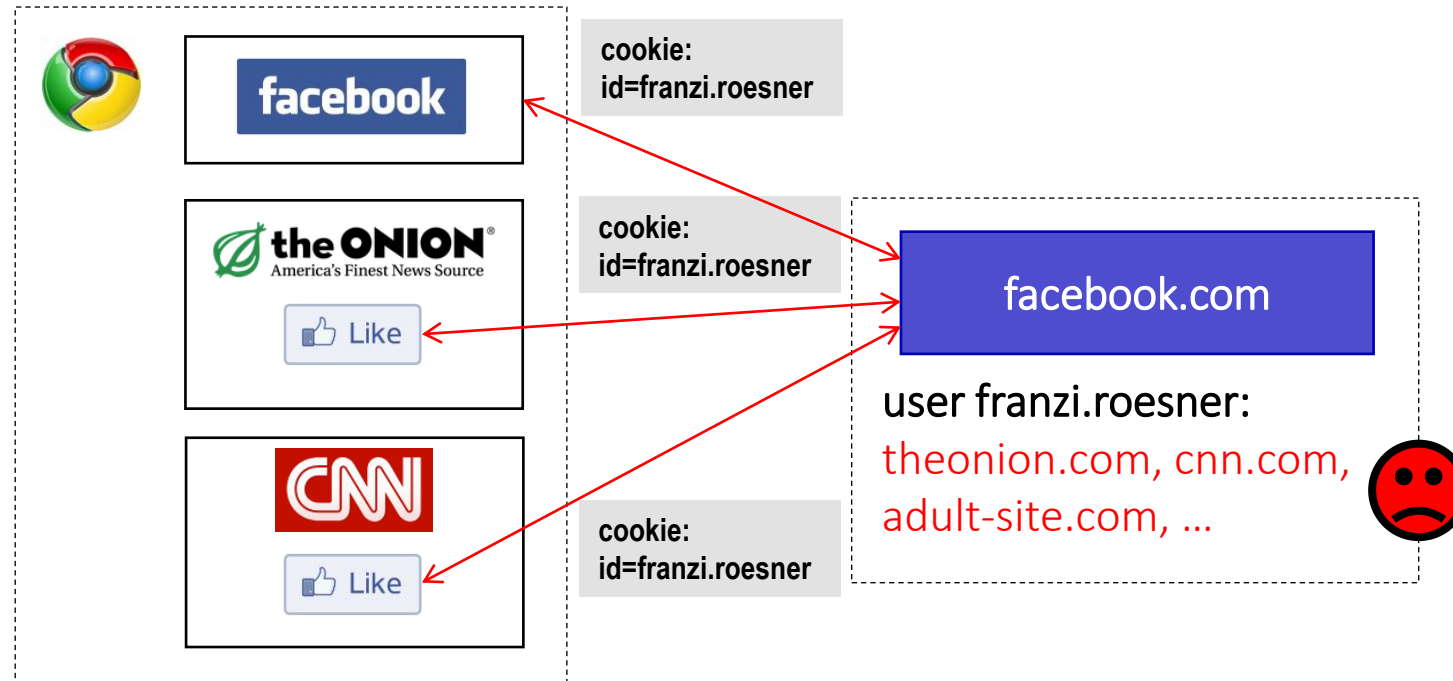
Other Trackers?



“Personal” Trackers



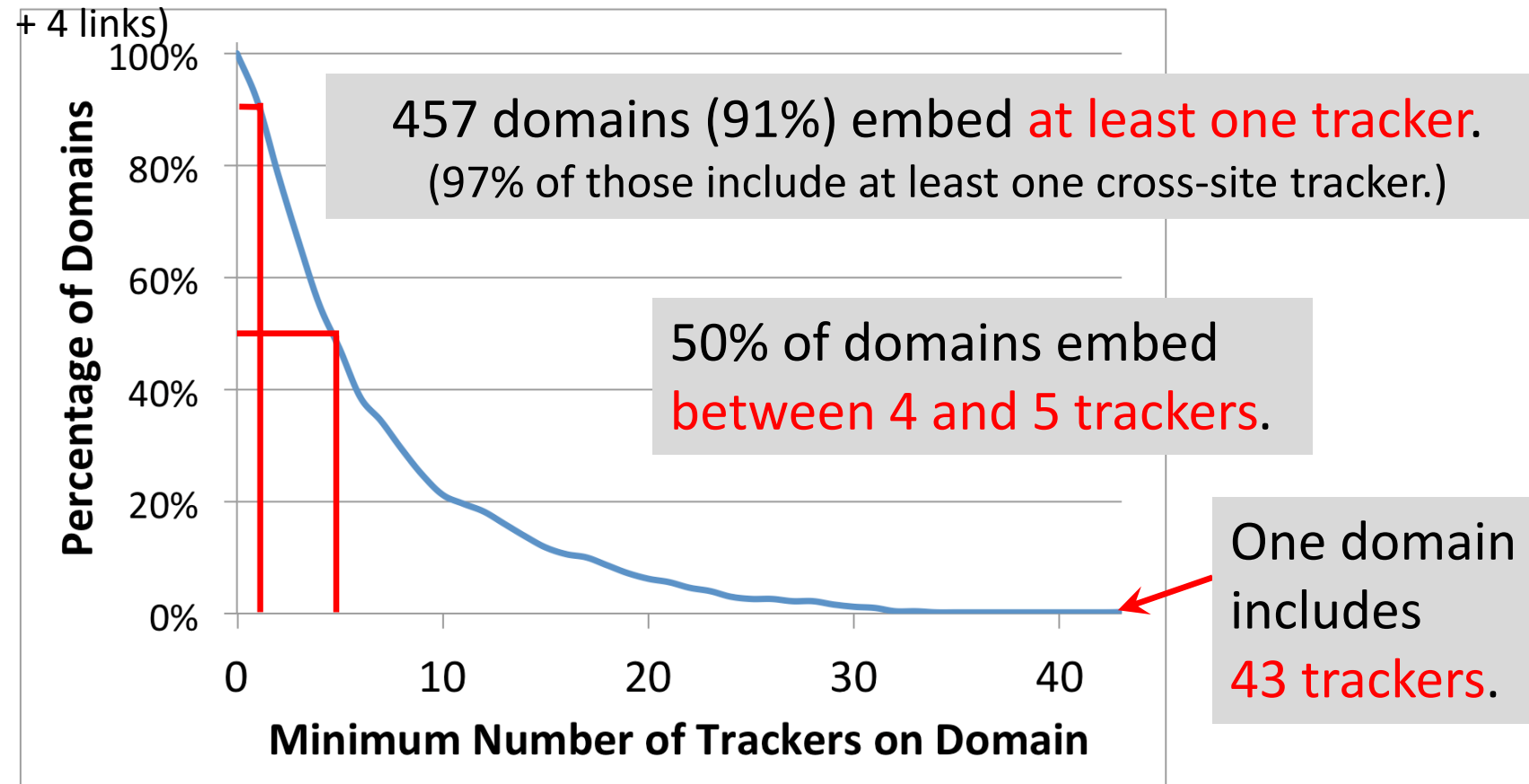
Personal Tracking



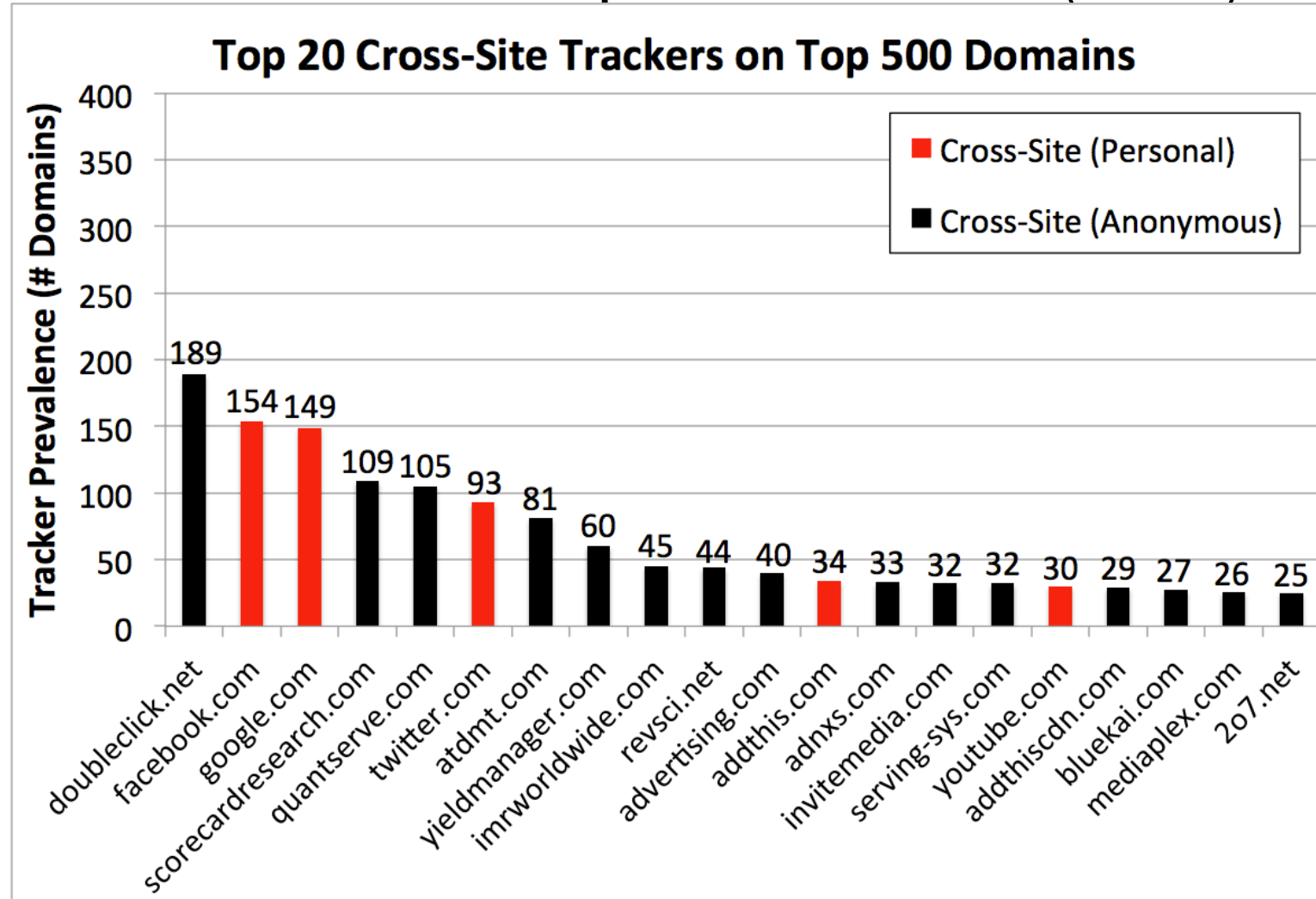
- Tracking is **not anonymous** (linked to accounts).
- Users **directly visit tracker's site** → evades some defenses.

How prevalent is tracking? (2011)

524 unique trackers on Alexa top 500 websites (homepages)



Who/what are the top trackers? (2011)

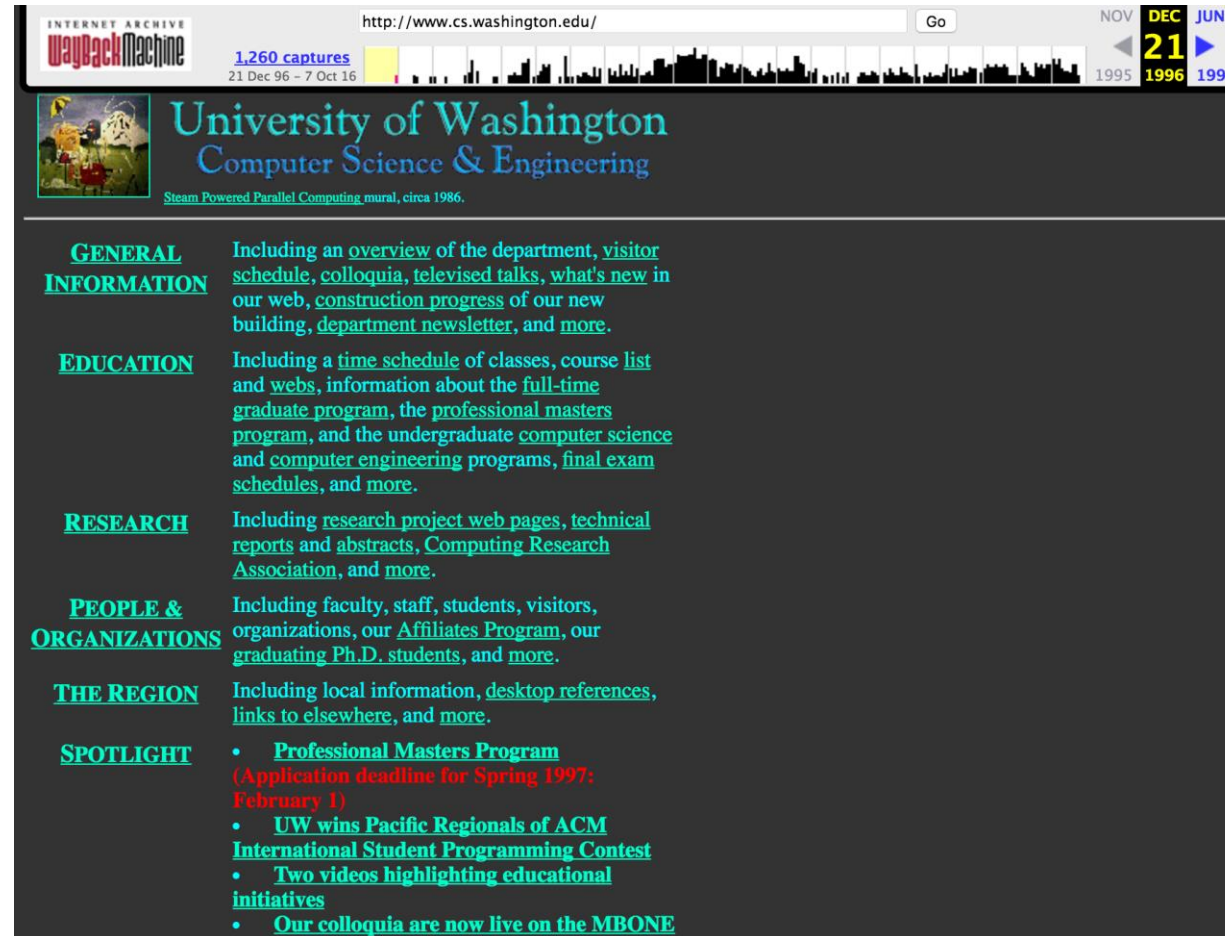


How has this changed over time?

- The web has existed for a while now...
 - What about tracking before 2011?
 - What about tracking before 2009?
- Solution: time travel!



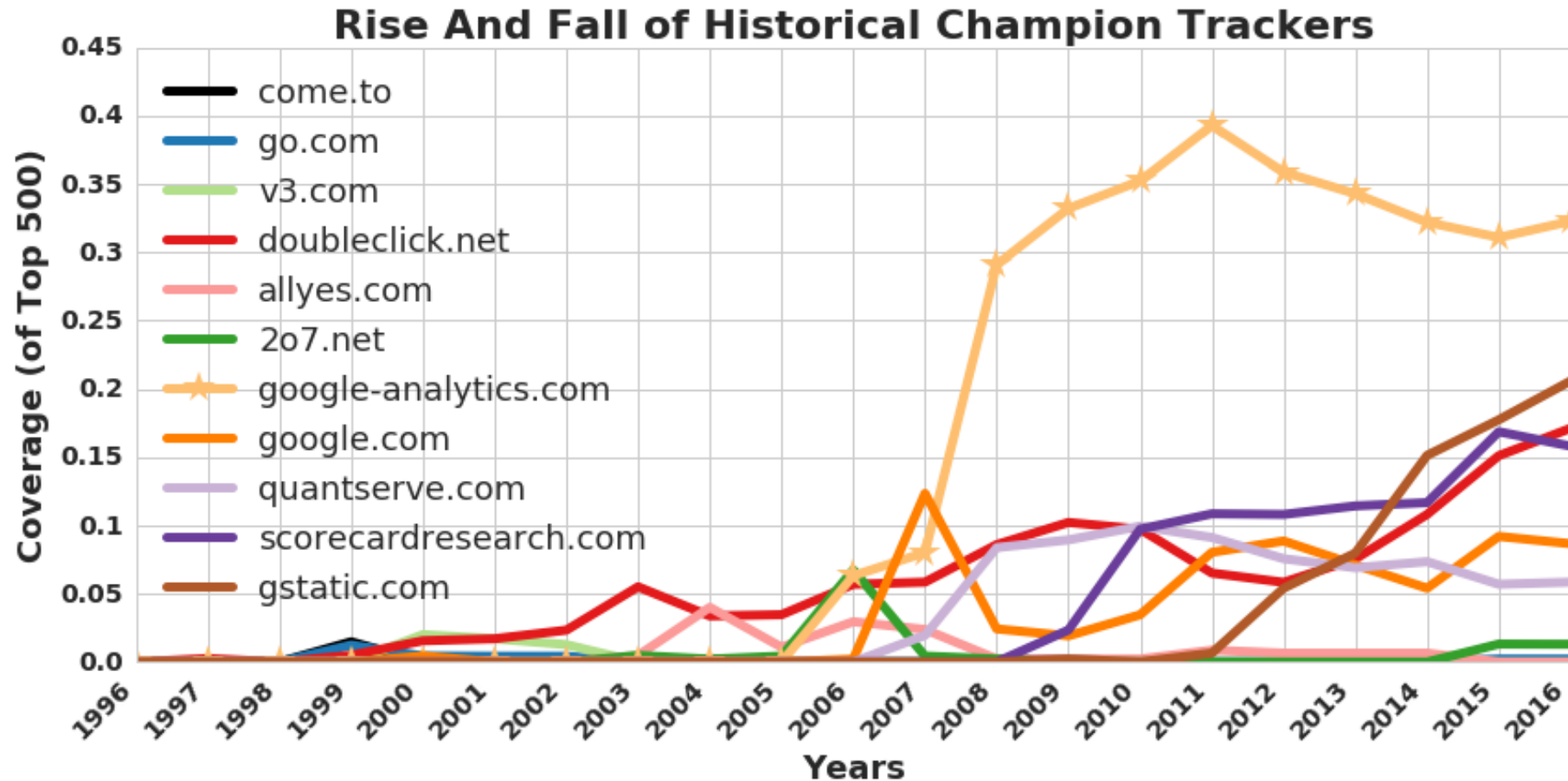
The Wayback Machine to the Rescue



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 protects against local, not network, attackers.

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:

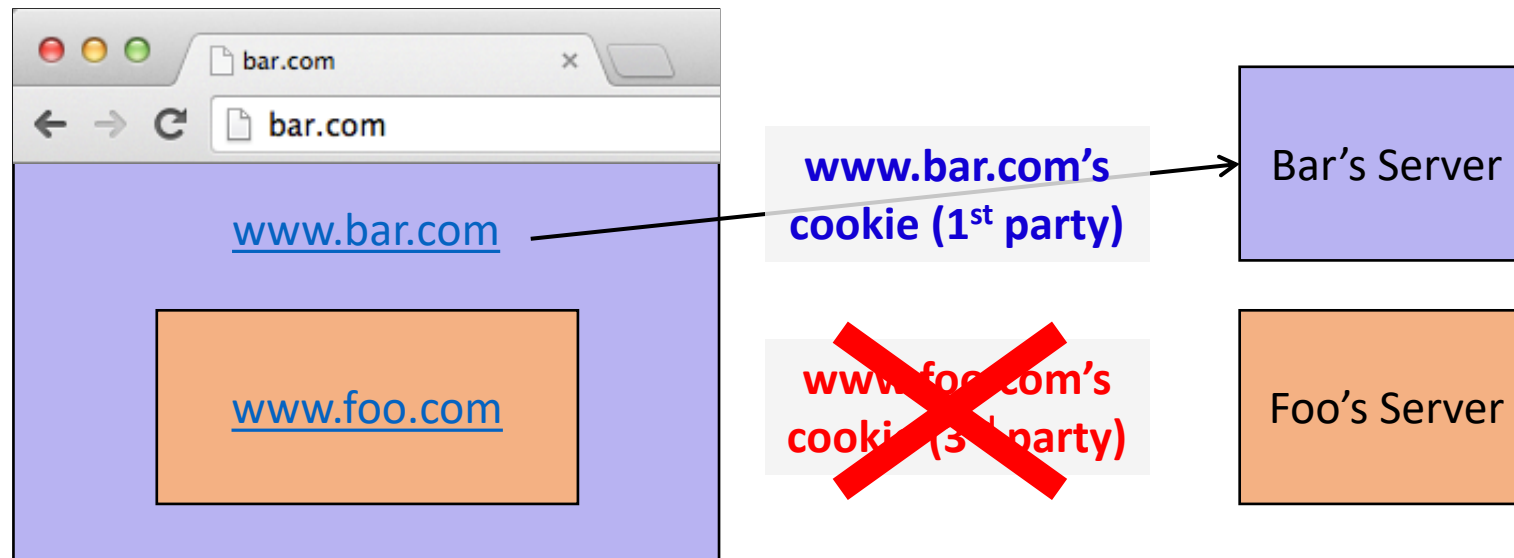
- Your browsing history
- Cookies and site data
- Information entered in forms

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?



Its real!

- 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.”

Fingerprinting is out there

- Better than a ‘voluntary’ cookie: involuntary, unchangeable id!
 - “Fingerprint”
- Idea: Measure ‘behavior’ of browser
 - Smash into unique ID

Fingerprinting Web Browsers

- User agent
- HTTP ACCEPT headers
- Browser plug-ins
- MIME support
- Clock skew
- Installed fonts
- Cookies enabled?
- Browser add-ons
- Screen resolution
- HTML5 canvas
(differences in graphics
SW/HW!)

HTML5 Canvas Fingerprinting - Text

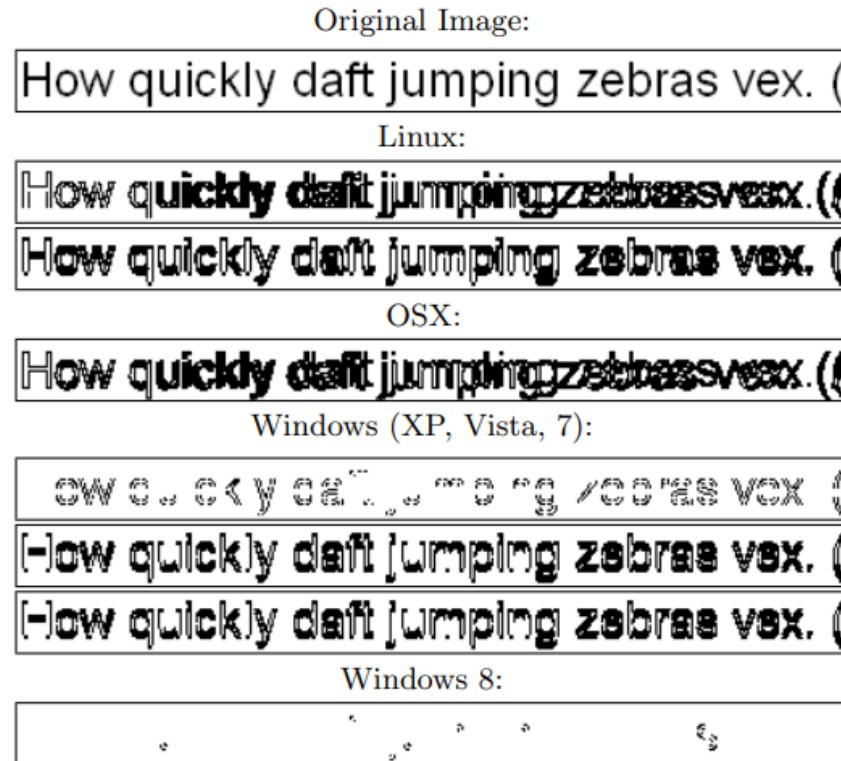


Figure 7: Difference maps for a group on `text_arial`

Mowery and Shacham, 2012

HTML5 Canvas Fingerprinting - Image

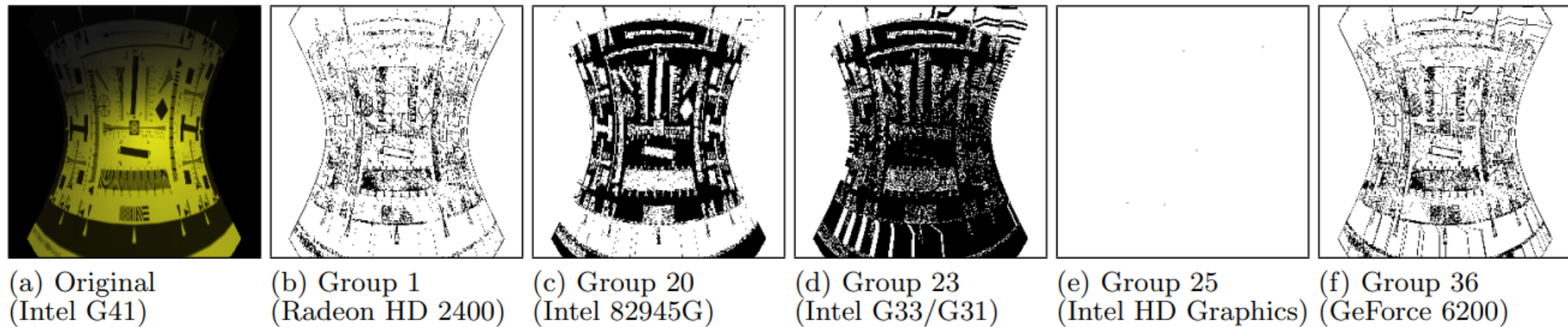


Figure 10: Original render and difference maps for Group 24

Mowery and Shacham, 2012

And its out there!



Figure 4: Different images printed to canvas by fingerprinting scripts. Note that the phrase “*Cwm fjordbank glyphs vext quiz*” in the top image is a *perfect pangram*, that is, it contains all the letters of the English alphabet only once to maximize diversity of the outcomes with the shortest possible string.

Fingerprinting Web Browsers

- User agent
- HTTP ACCEPT headers
- Browser plug-ins
- MIME support
- Clock skew
- Installed fonts
- Cookies enabled?
- Browser add-ons
- Screen resolution
- HTML5 canvas
(differences in graphics
SW/HW!)

COVER YOUR TRACKS

See how trackers view your browser

[Learn](#)

[About](#)

HOW TO READ YOUR REPORT

You will see a summary of your overall tracking protection. The first section gives you a general idea of what your browser configuration is blocking (or not blocking). Below that is a list of specific browser characteristics in the format that a tracker would view them. We also provide descriptions of how they are incorporated into your fingerprint.

HOW CAN TRACKERS TRACK YOU?

Trackers use a variety of methods to identify and track users. Most often, this includes tracking cookies, but it can also include browser fingerprinting. Fingerprinting is a sneakier way to track users and makes it harder for users to regain control of their browsers. This report measures how easily trackers might be able to fingerprint your browser.

HOW CAN I USE MY RESULTS TO BE MORE ANONYMOUS?

Knowing how identifiable you are, or whether you are blocking trackers, can help you take steps to better protect your privacy. Browser add-ons or protection mechanisms built into the browser can help. Even so, the sneakiest trackers have ways around even the strongest security.

Here are your Cover Your Tracks results. They include an overview of how visible you are to trackers, with an index (and glossary) of all the metrics we measure below.

Our tests indicate that you have strong protection against Web tracking.

IS YOUR BROWSER:

Blocking tracking ads?	<u>Yes</u>
Blocking invisible trackers?	<u>Yes</u>
Protecting you from <u>fingerprinting</u> ?	<u>Your browser has a nearly-unique fingerprint</u>

Still wondering how fingerprinting works?

[LEARN MORE](#)

Note: because
tracking and p

Your R

One in 145,235 browsers have
the same fingerprint

measure all forms of

Within our dataset of several hundred thousand visitors tested in the past 45 days, only **one in 145,235.5 browsers have the same fingerprint as yours.**

Fingerprinting as a security measure

- Blocking bots (e.g. reCAPTCHA)
- Validating users over-time

How should we view tracking and fingerprinting efforts?

“Privacy preserving” personalized ads

- <https://github.com/WICG/turtledove>
 - The browser, not the advertiser, holds the information about what the advertiser thinks a person is interested in.
 - Advertisers can serve ads based on an interest, but cannot combine that interest with other information about the person — in particular, with who they are or what page they are visiting.
 - Web sites the person visits, and the ad networks those sites use, cannot learn about their visitors' ad interests.