CSE 484: Computer Security and Privacy

Web Tracking and Physical Security

Spring 2021

Tadayoshi Kohno

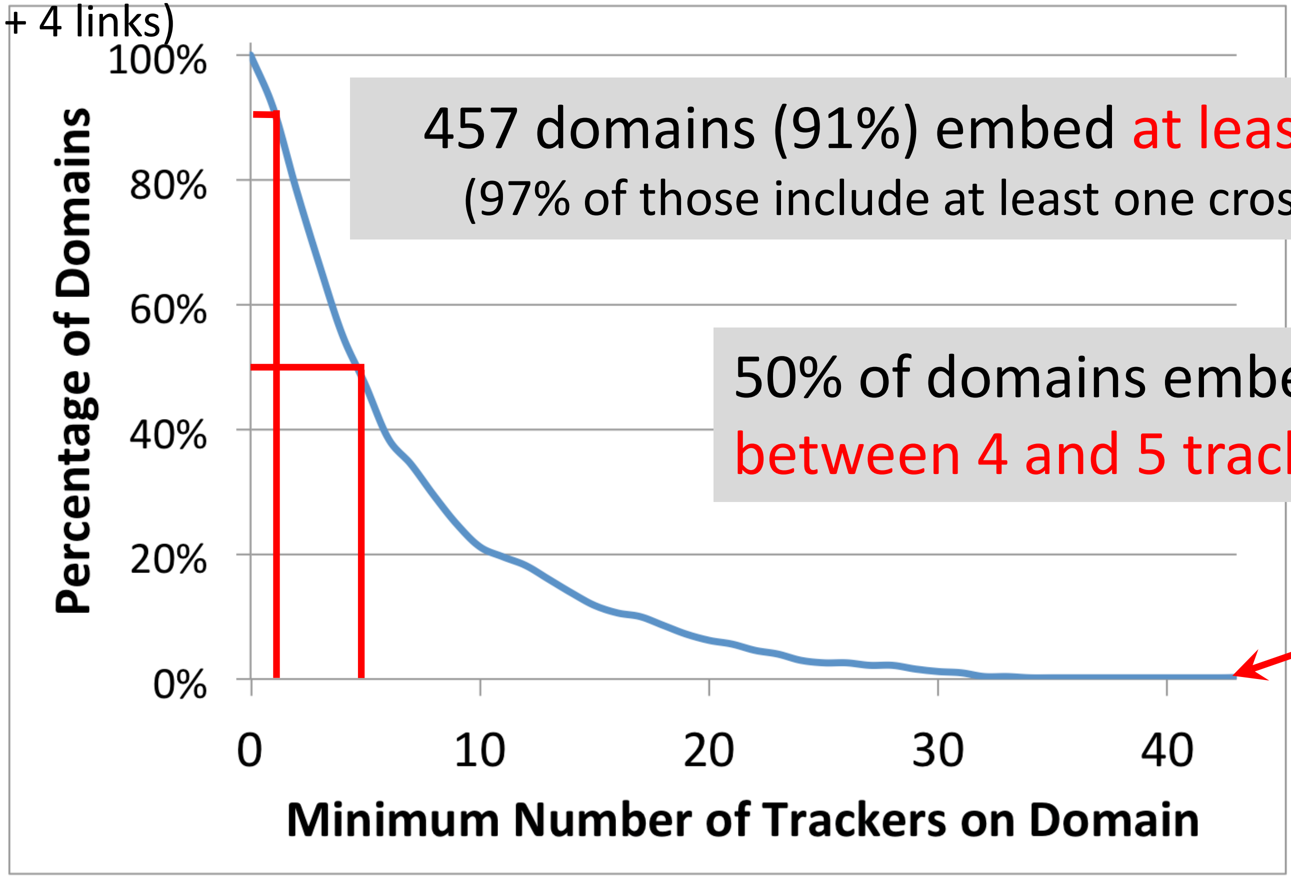
Thanks to Franzi Roesner, Dan Boneh, Dieter Gollmann, Dan Halperin, David Kohlbrenner, Yoshi Kohno, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Administrivia

- Lab 2 due May 25 → May 27
- Final Project Checkpoint due May 26
- Friday (May 28): Guest Lecture: Charlie Reis (Google)

How prevalent is tracking? (2011)

524 unique trackers on Alexa top 500 websites (homepages + 4 links)

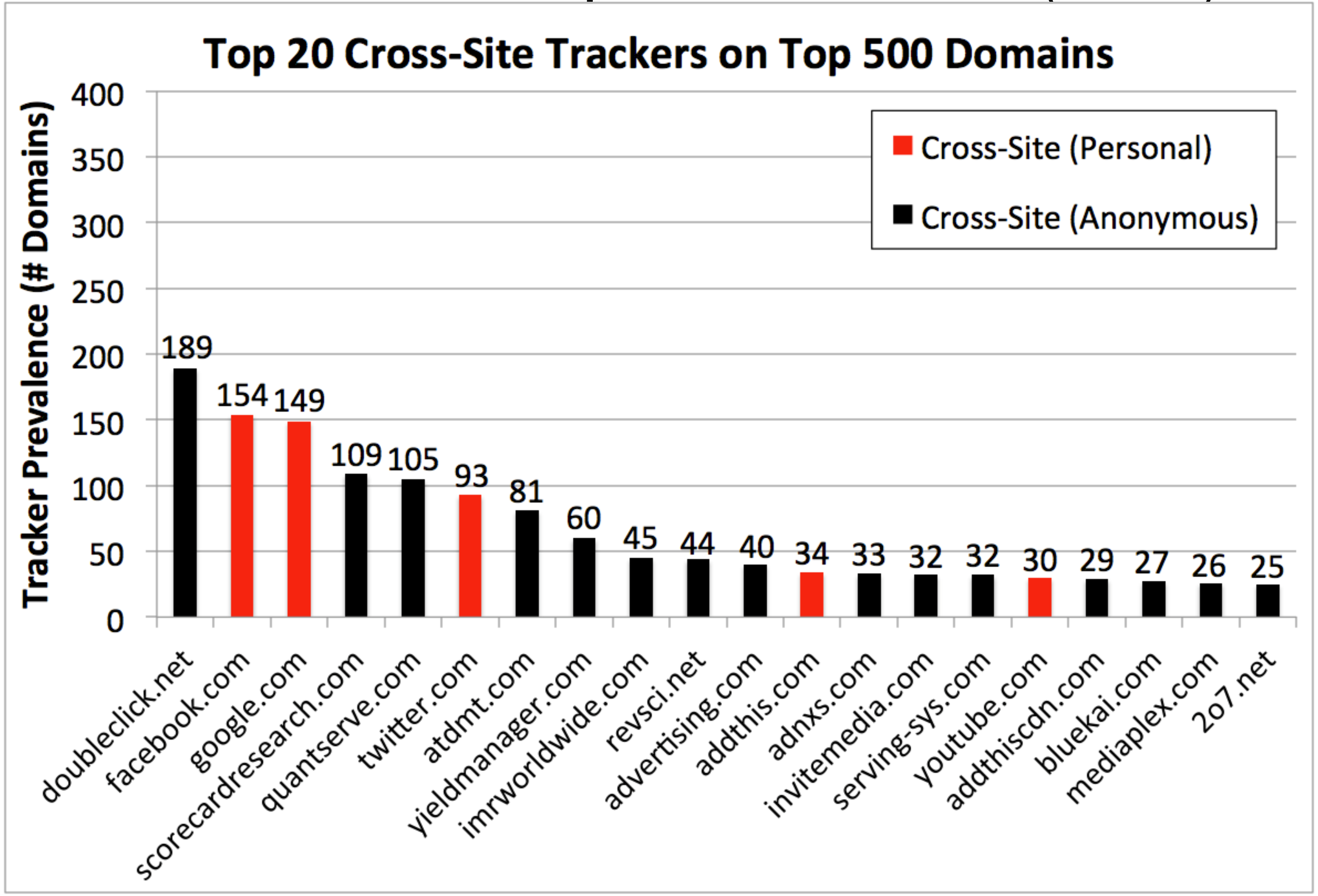


457 domains (91%) embed at least one tracker.
(97% of those include at least one cross-site tracker.)

50% of domains embed between 4 and 5 trackers.

One domain includes 43 trackers.

Who/what are the top trackers? (2011)

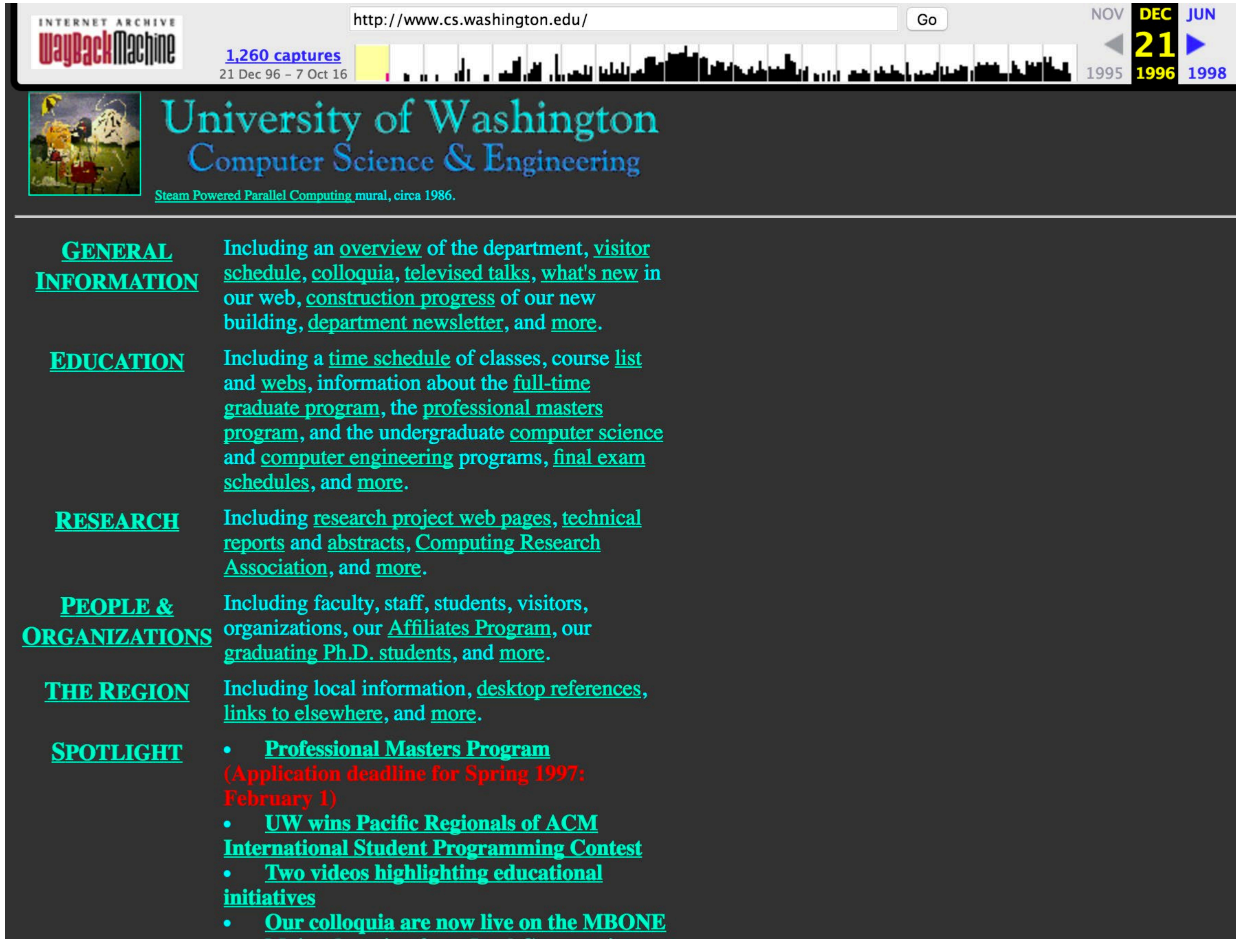


How has this changed over time?

- 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



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.

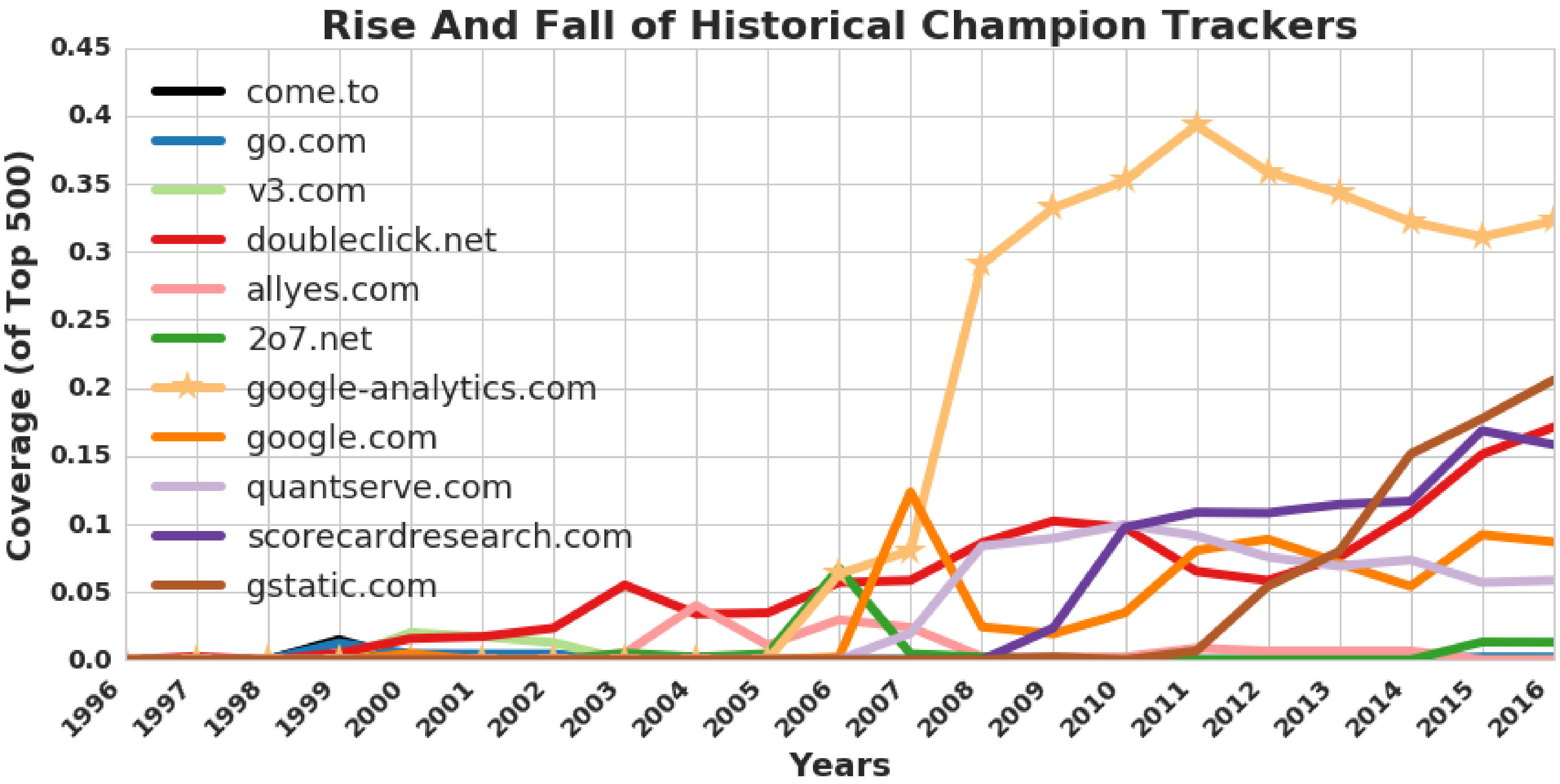
SPOTLIGHT

- **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

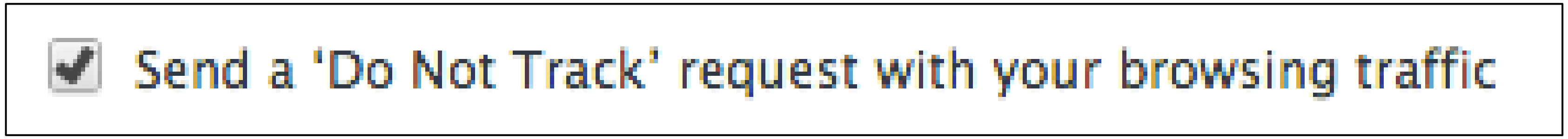
1996-2016: More & More Tracking

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



Defenses to Reduce Tracking

- Do Not Track?



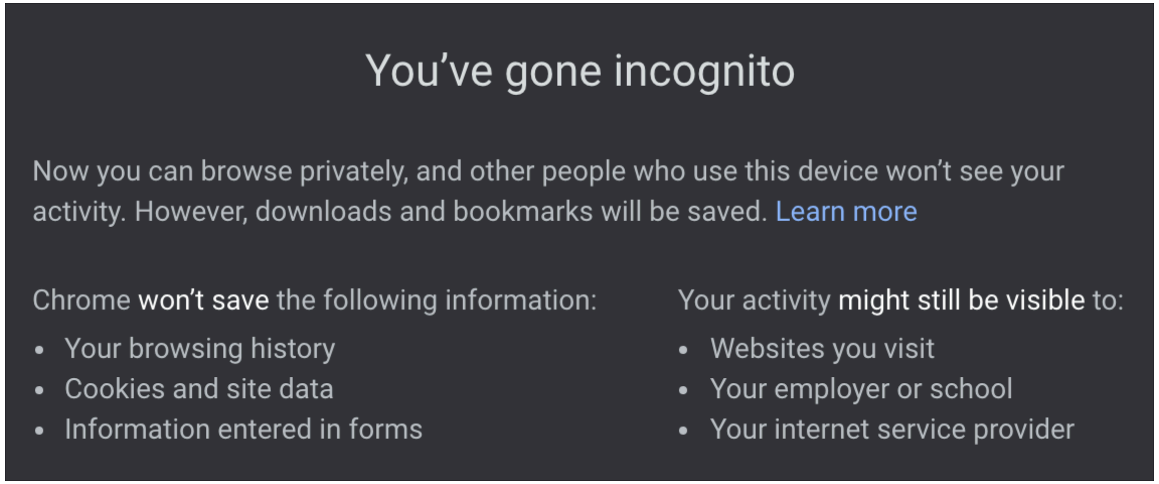
☑ Send a 'Do Not Track' request with your browsing traffic

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 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:

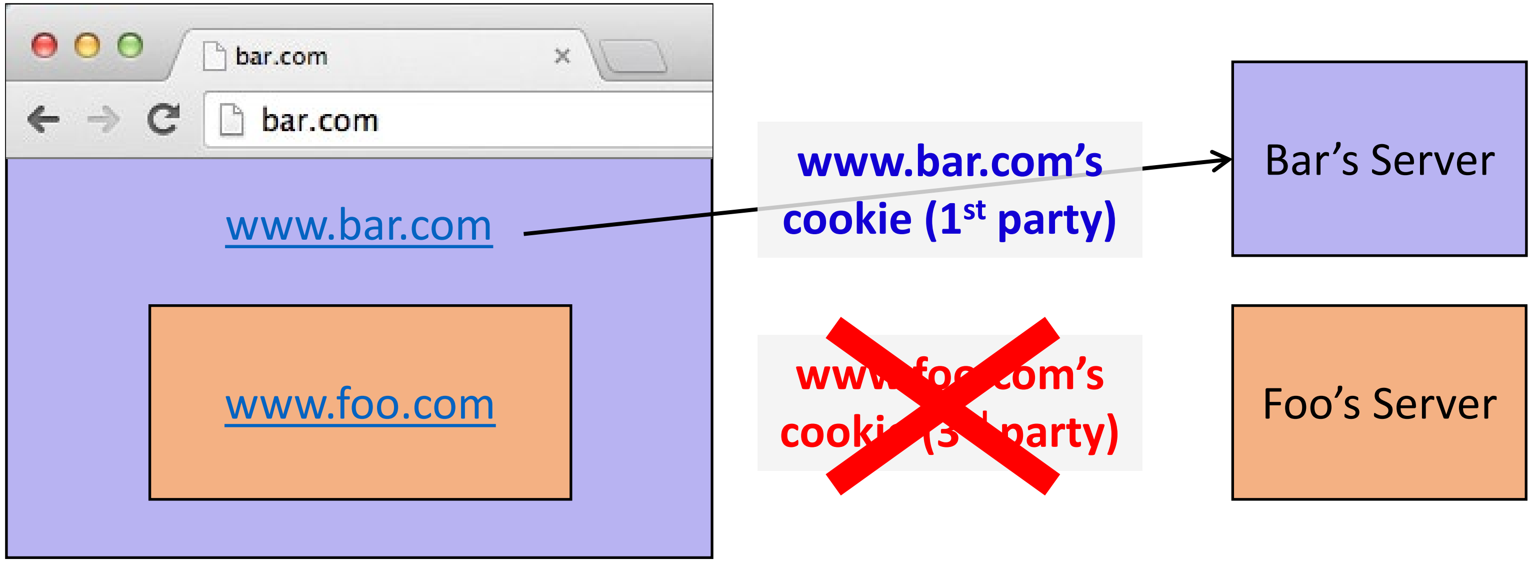
- Your browsing history
- Cookies and site data
- Information entered in forms

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?



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

Its real!

- Safari and FF 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:
  - Older quote: "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."
  - January 2021 article: Start removing in ~April 2021: https://www.pcmag.com/news/google-effort-to-kill-third-party-cookies-in-chrome-rolls-out-in-april

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

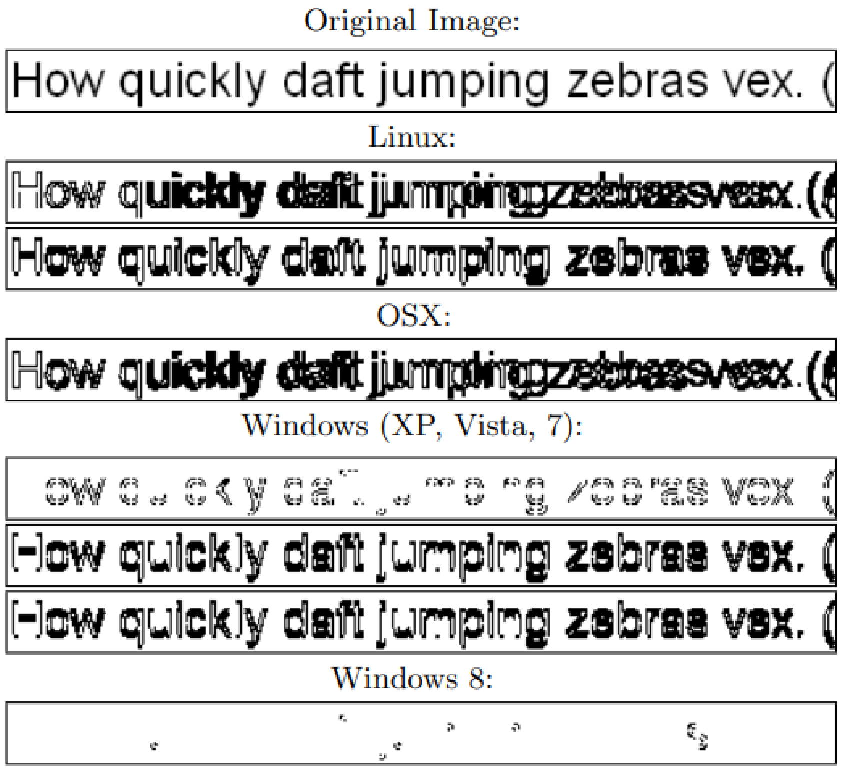
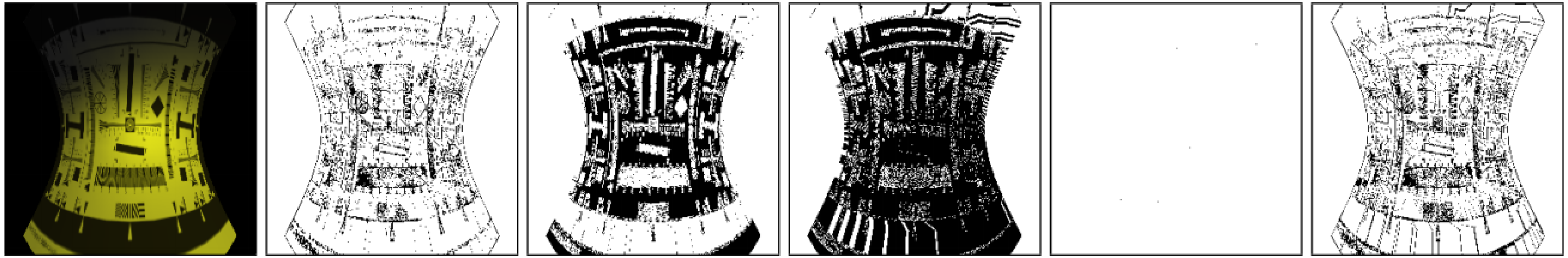


Figure 7: Difference maps for a group on `text_arial`

Mowery and Shacham, 2012

HTML5 Canvas Fingerprinting - Image



(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)

Figure 10: Original render and difference maps for Group 24

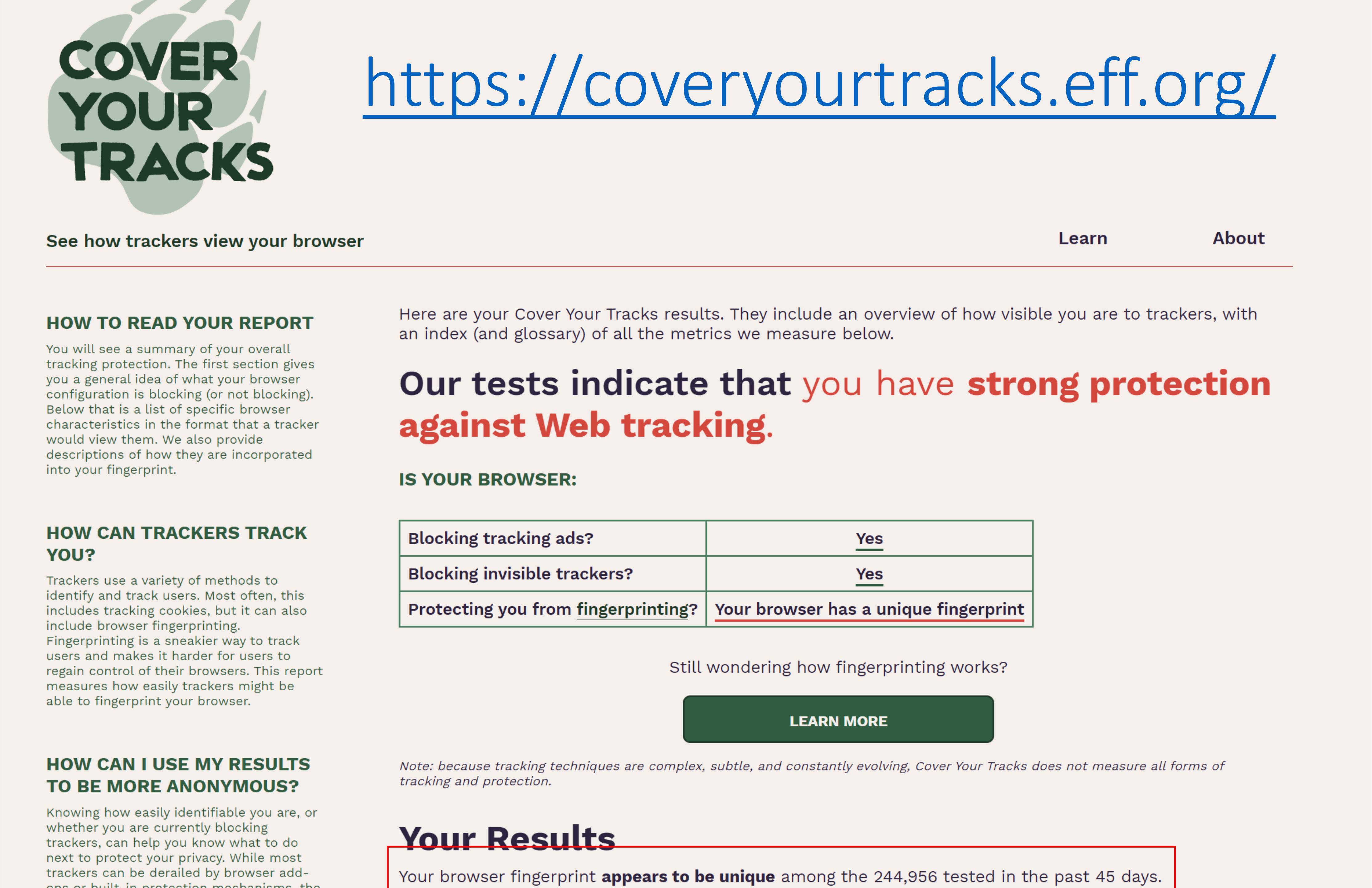
Mowery and Shacham, 2012

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!)

https://coveryourtracks.eff.org/



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 easily identifiable you are, or whether you are currently blocking trackers, can help you know what to do next to protect your privacy. While most trackers can be derailed by browser add-ons or built-in protection mechanisms, the

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?	Yes
Blocking invisible trackers?	Yes
Protecting you from fingerprinting?	Your browser has a unique fingerprint

Still wondering how fingerprinting works?

LEARN MORE

Note: because tracking techniques are complex, subtle, and constantly evolving, Cover Your Tracks does not measure all forms of tracking and protection.

Your Results

Your browser fingerprint **appears to be unique** among the 244,956 tested in the past 45 days.

Fingerprinting as a security measure

- Blocking bots (e.g., reCAPTCHA)

- Validating credit card transactions

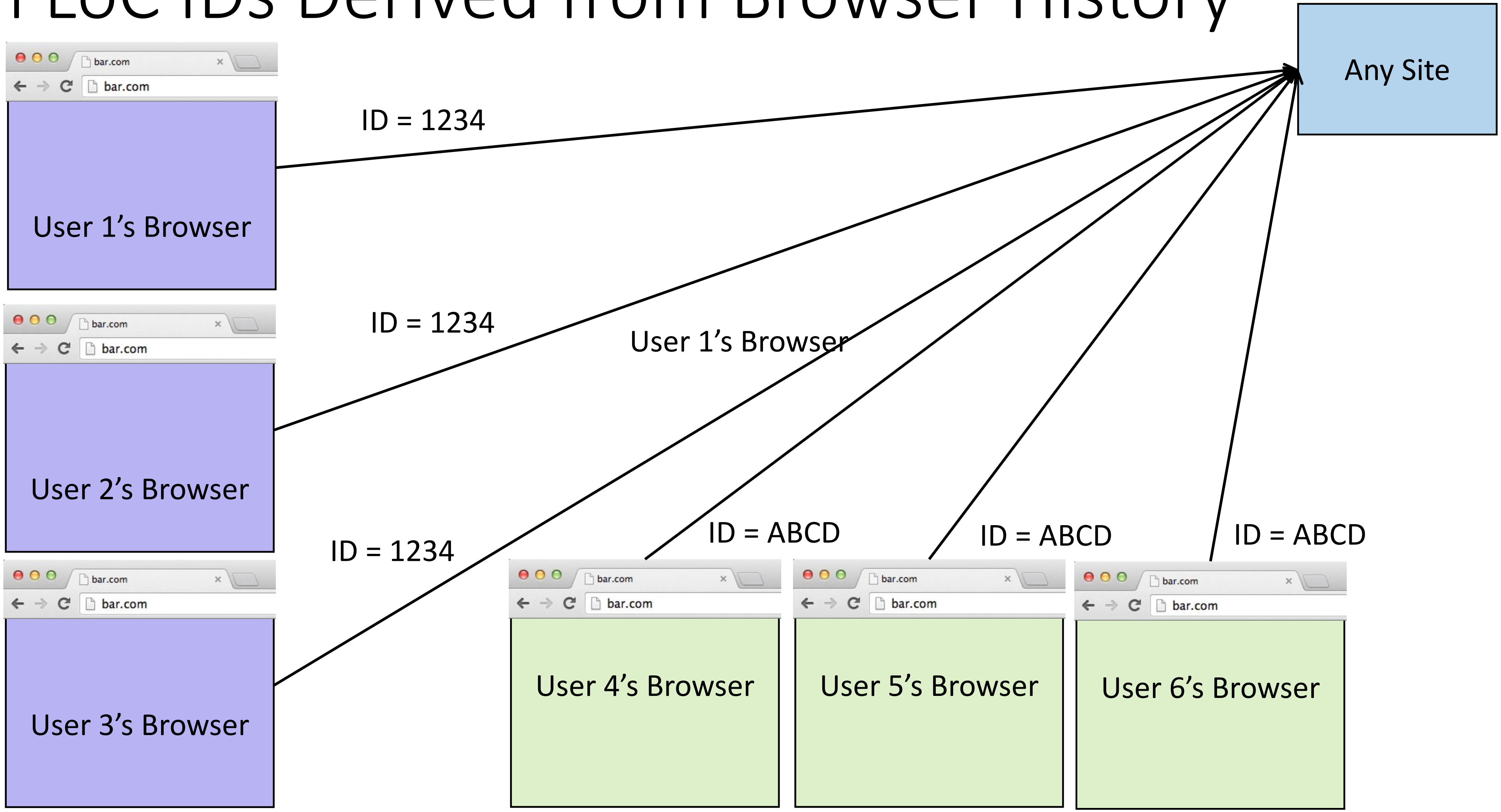
- Validating users over-time

Federated Learning of Cohorts (FLoC)

- Stop: Tracking individual browsers / users
- Start: Tracking cohorts (groups) of browsers / users
- Derive cohort ID (FLoC ID) based on last week of browser history
- Users with similar browsing profiles would have similar FLoC IDs

- Google / Chrome currently (Spring 2021) testing with small fraction of users (still many, many users)

FLoC IDs Derived from Browser History



New, Many Questions Remain

- Old 3rd-party cooky days: 1st party not learn information about browsing history (unless 3rd-party reveals that information)
- FLoC: 1st party learns FLoC ID
  - May not be big privacy risk for small sites with few users?
  - May be larger privacy risk for large sites, with many users (e.g., Facebook, Amazon)
  - Emphasis on word “may”: Lots of unknowns

New, Many Questions Remain

- Web Incubator CG / FLoC: https://github.com/WICG/floc
- EFF, March 2021: Google's FLoC is a Terrible Idea: https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea
  - "**The technology will avoid the privacy risks of third-party cookies, but it will create new ones in the process**. It may also **exacerbate many of the worst non-privacy problems with behavioral ads, including discrimination and predatory targeting.**"
  - "FLoC is part of a suite **intended to bring targeted ads into a privacy-preserving future**. But **the core design involves sharing new information with advertisers**. Unsurprisingly, **this also creates new privacy risks**."

Discussion of FLoC

Physical security

Physical Security and Computer Security

- Relate physical security to computer security
  - Locks, safes, etc
- Why?
  - More similar than one might think!!
  - The more places one sees “the Security Mindset” and security issues manifest, the more opportunities “the Security Mindset Muscle” can grow
  - After CSE 484, please do try to keep thinking about security everywhere – computers, locks, windows, …
    - Of course, take a balanced perspective, consider risk management, and note that “the sky is not falling” ☺

Switching Slide Decks

- We will switch to a slide deck that will not be online
- But if you're interested in the subject of lockpicking, see:
  - Blaze, "Cryptology and Physical Security: Rights Amplification in Master-Keyed Mechanical Locks"
  - Blaze, "Safecracking for the Computer Scientist"
  - Tool, "Guide to Lock Picking"
  - Tobias, "Opening Locks by Bumping in Five Seconds or Less"