CSE 484 / CSE M 584: Computer Security and Privacy

Web Security
[Web Privacy]

Autumn 2020

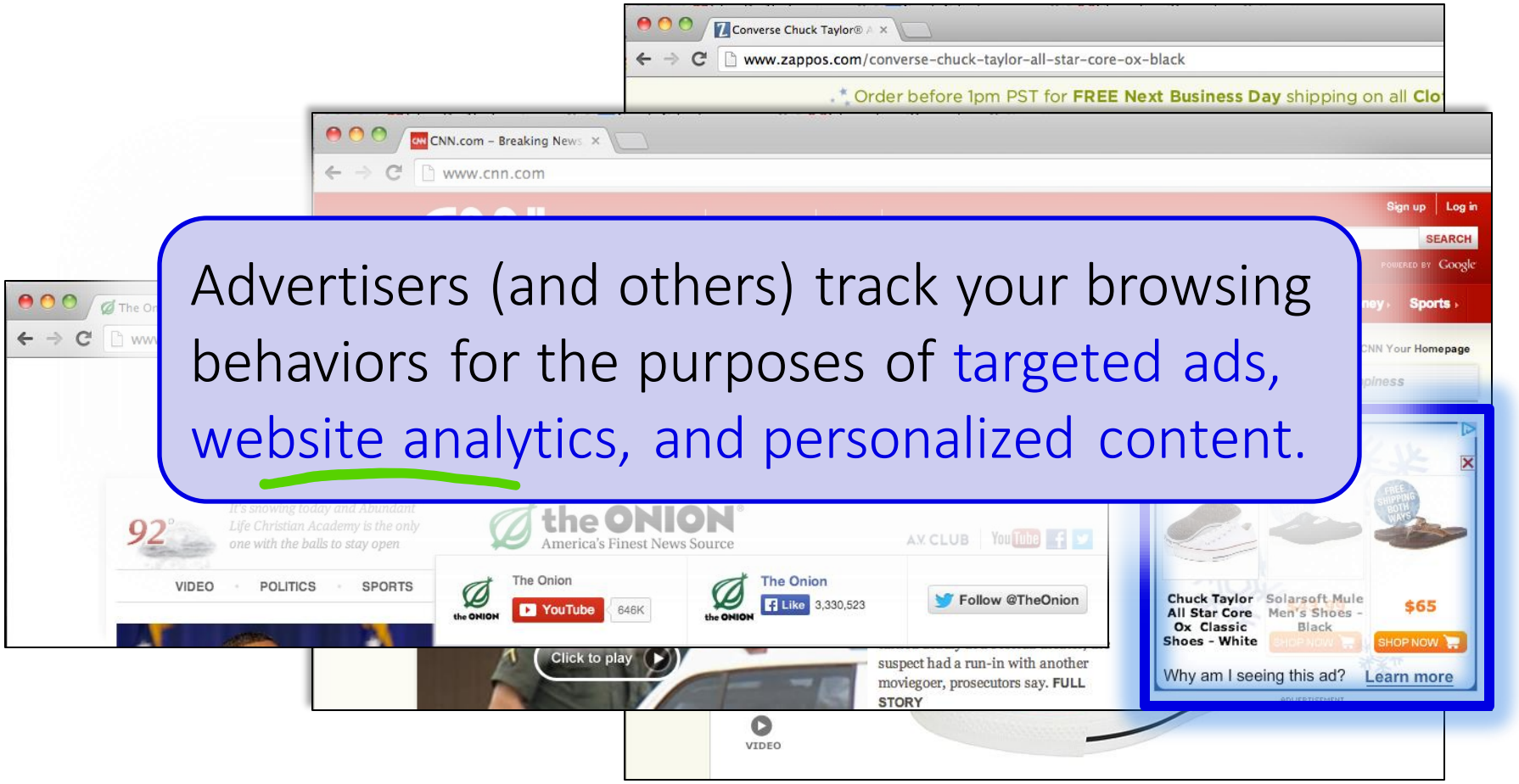
Franziska (Franzi) Roesner
franzi@cs.washington.edu

Thanks to 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

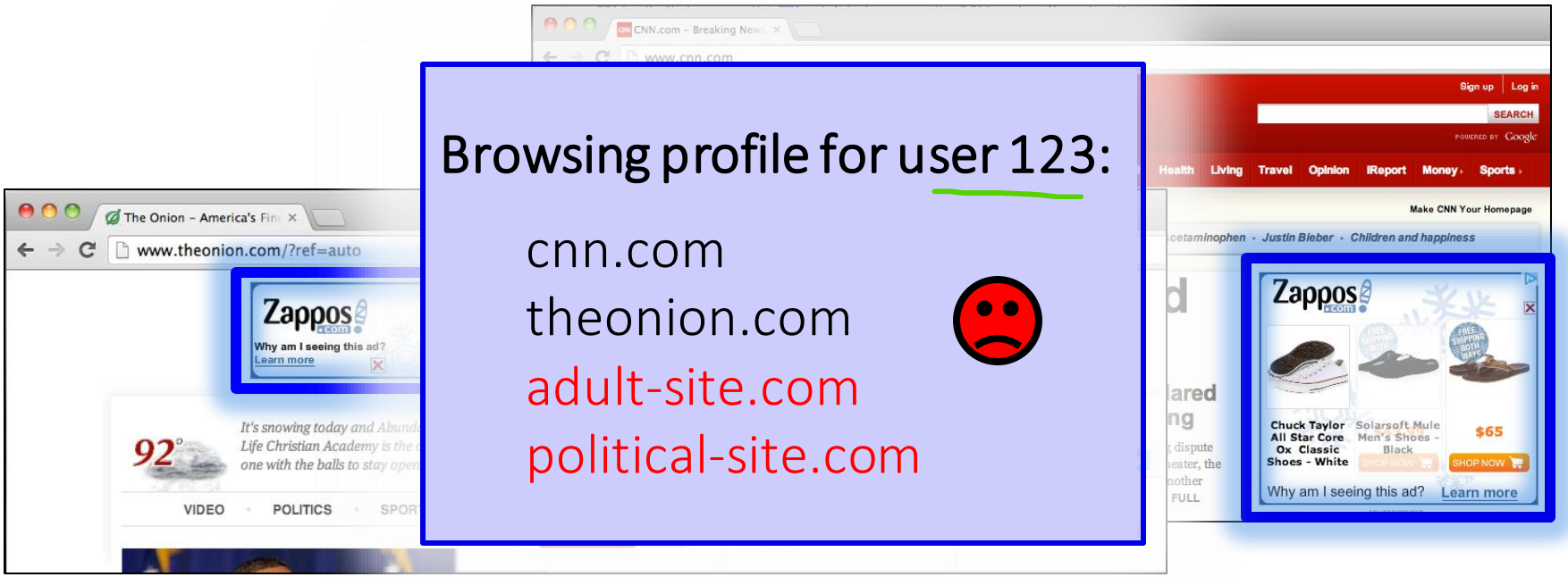
- Lab 2:
  - Check access ASAP
  - Read FAQs ☺
- Homework 3: out soon, due 12/4
- Guest lecture on Friday
  - Emily McReynolds, law & policy
- No class the day before Thanksgiving

Ads That Follow You



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

Third-Party Web Tracking



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

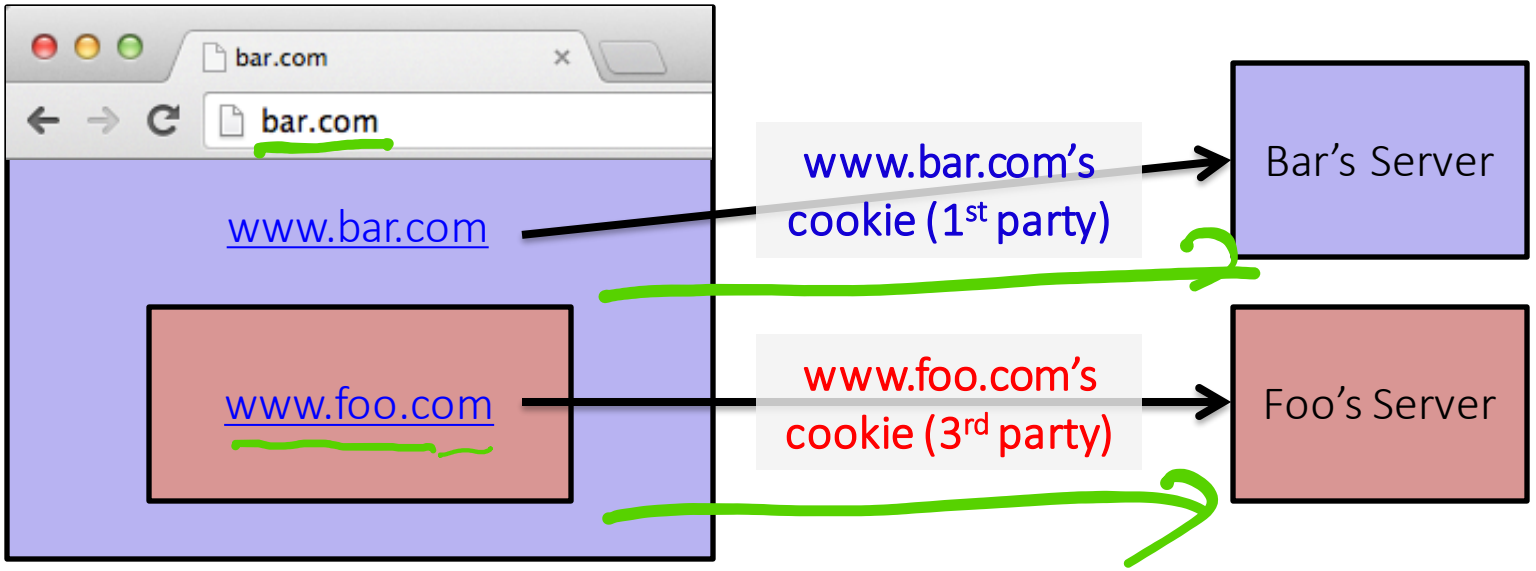
Concerns About Privacy

Outline

1. Understanding web tracking
2. Measuring web tracking
3. Defenses

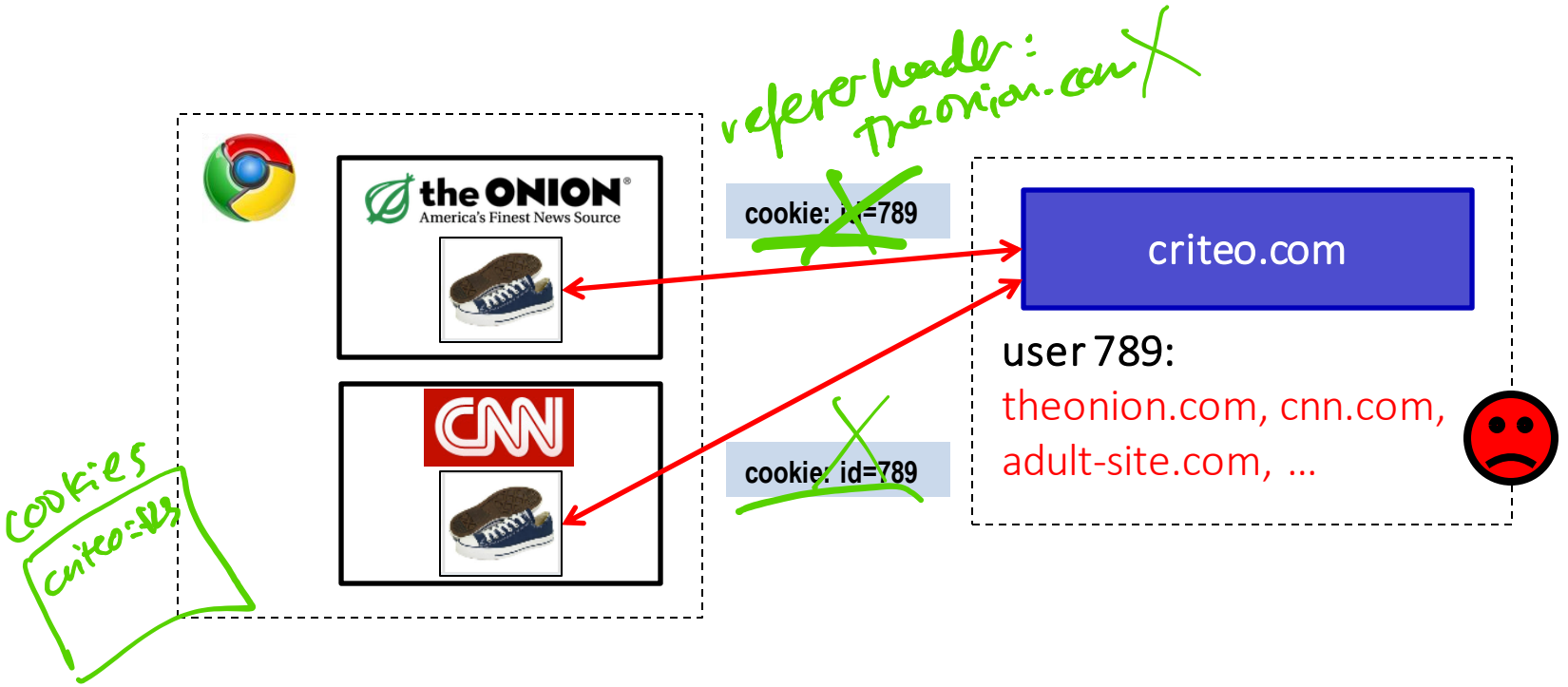
First and Third Parties

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



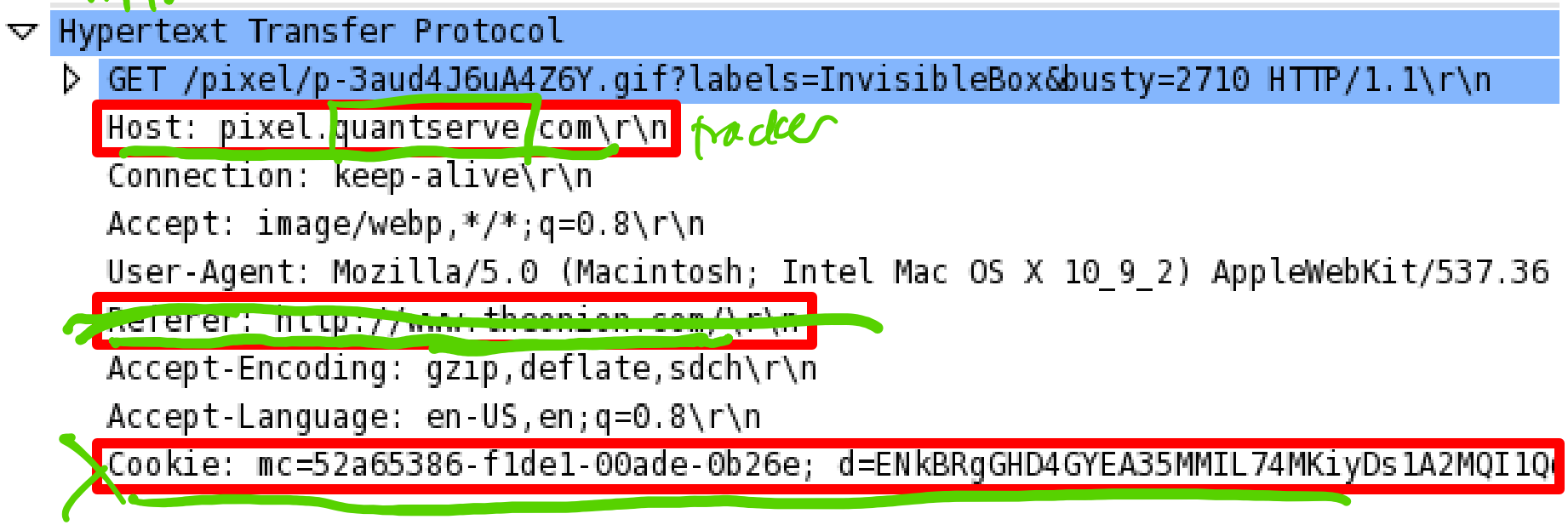
Anonymous Tracking

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

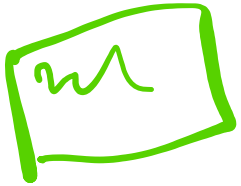
- Flash cookies
- Silverlight storage
- TLS session ID & resume
- Browsing history
- window.name
- HTTP STS
- DNS cache

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

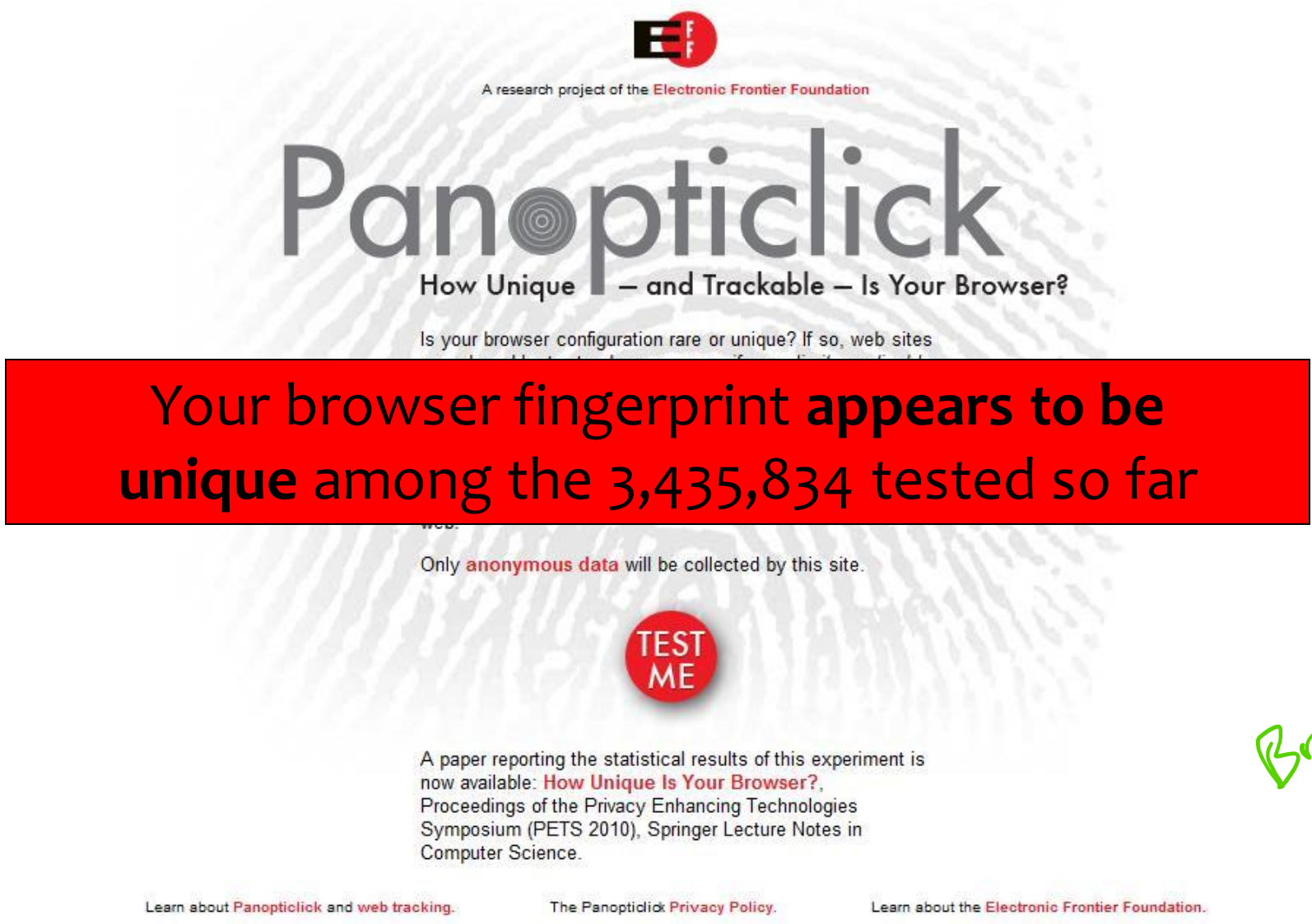
Fingerprinting Web Browsers

- 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!)



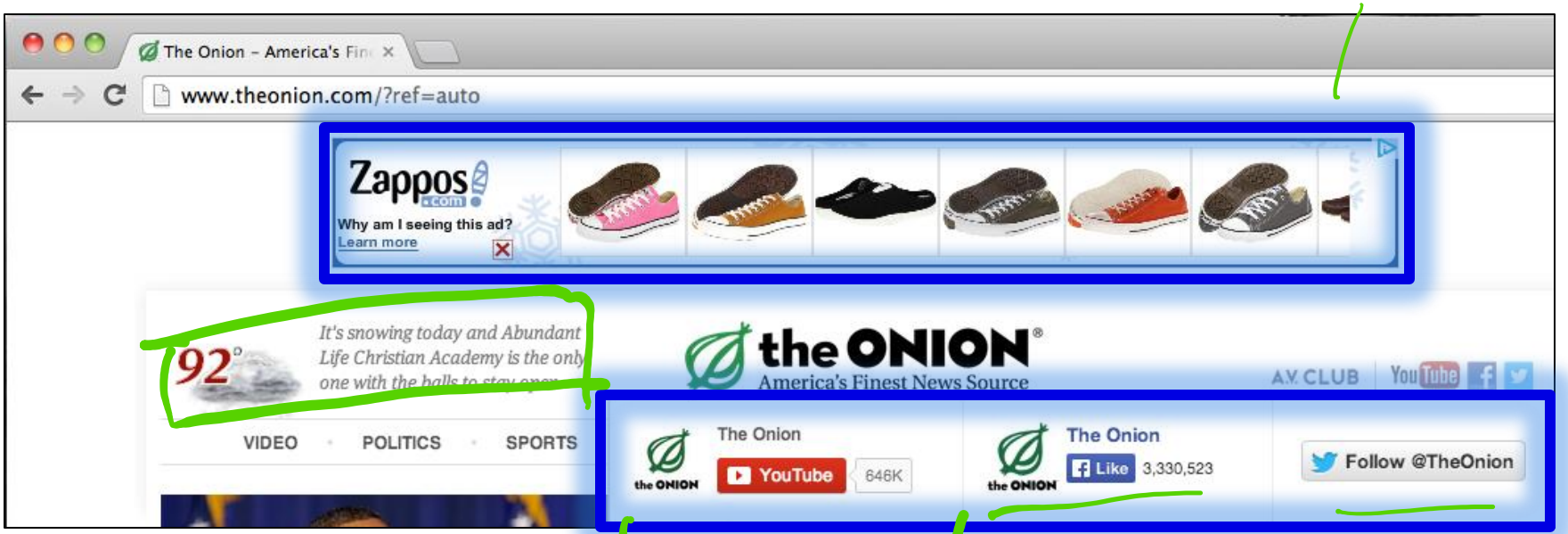
panopticlick.eff.org



Brave

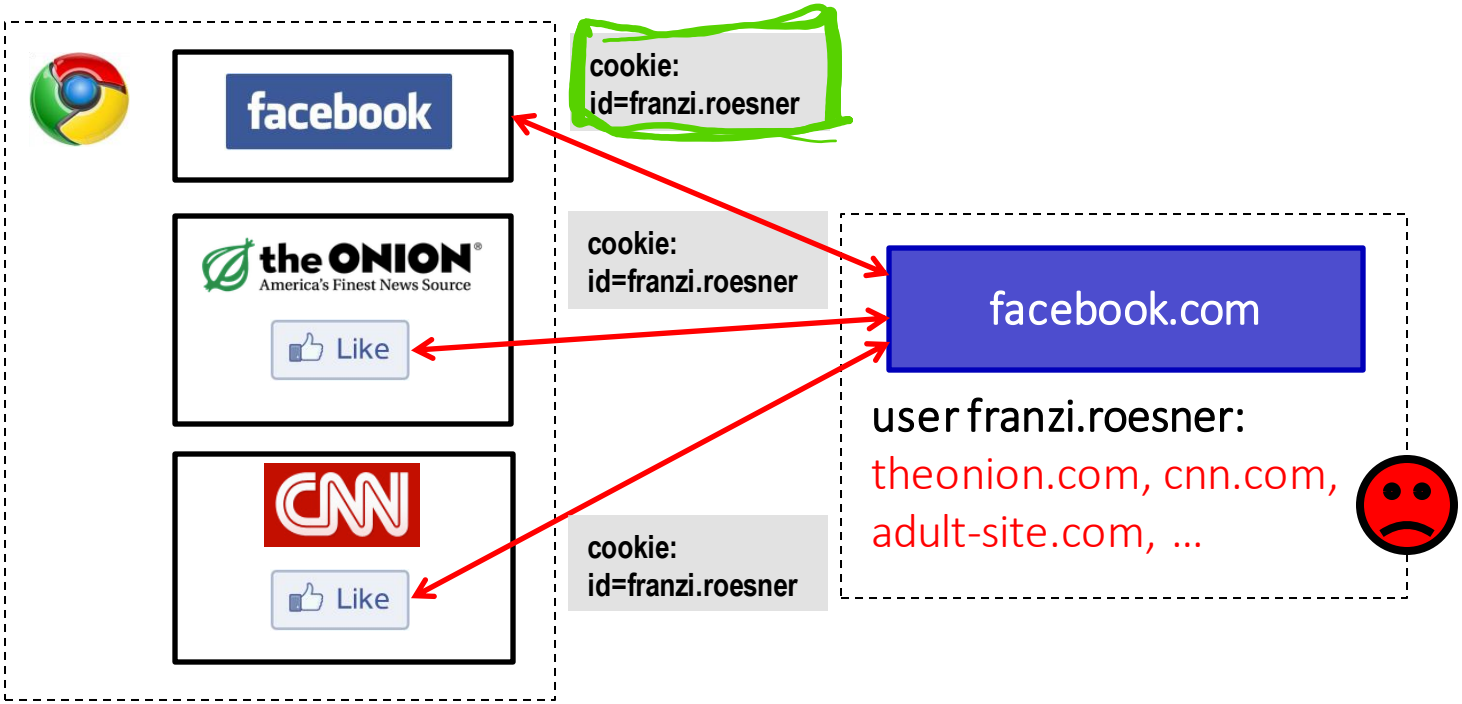
Other Trackers?

criteo



"Personal" Trackers

Personal Tracking



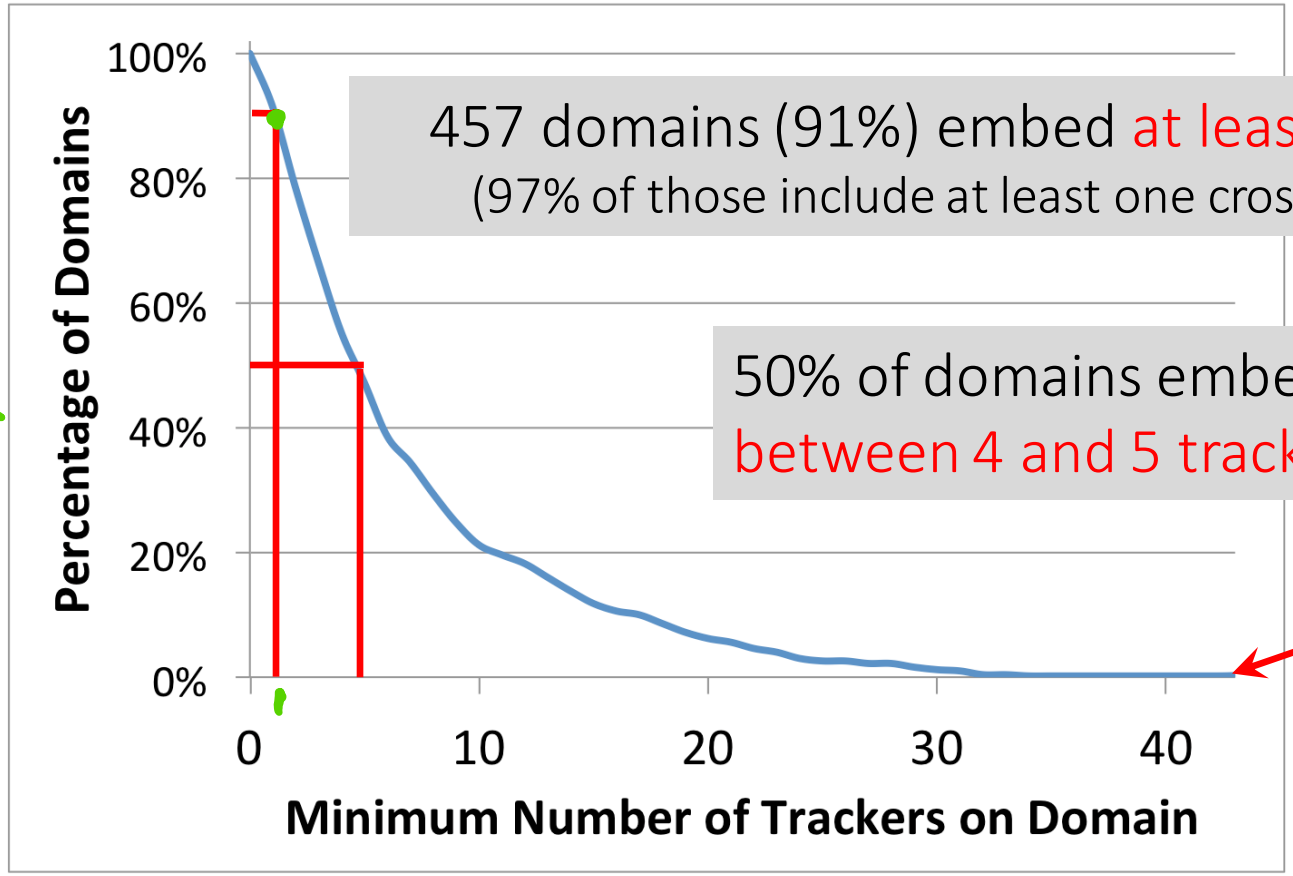
- Tracking is not anonymous (linked to accounts).
- Users directly visit tracker's site → evades some defenses.

Outline

1. Understanding web tracking
2. Measuring web tracking
3. Defenses

How prevalent is tracking? (2011)

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

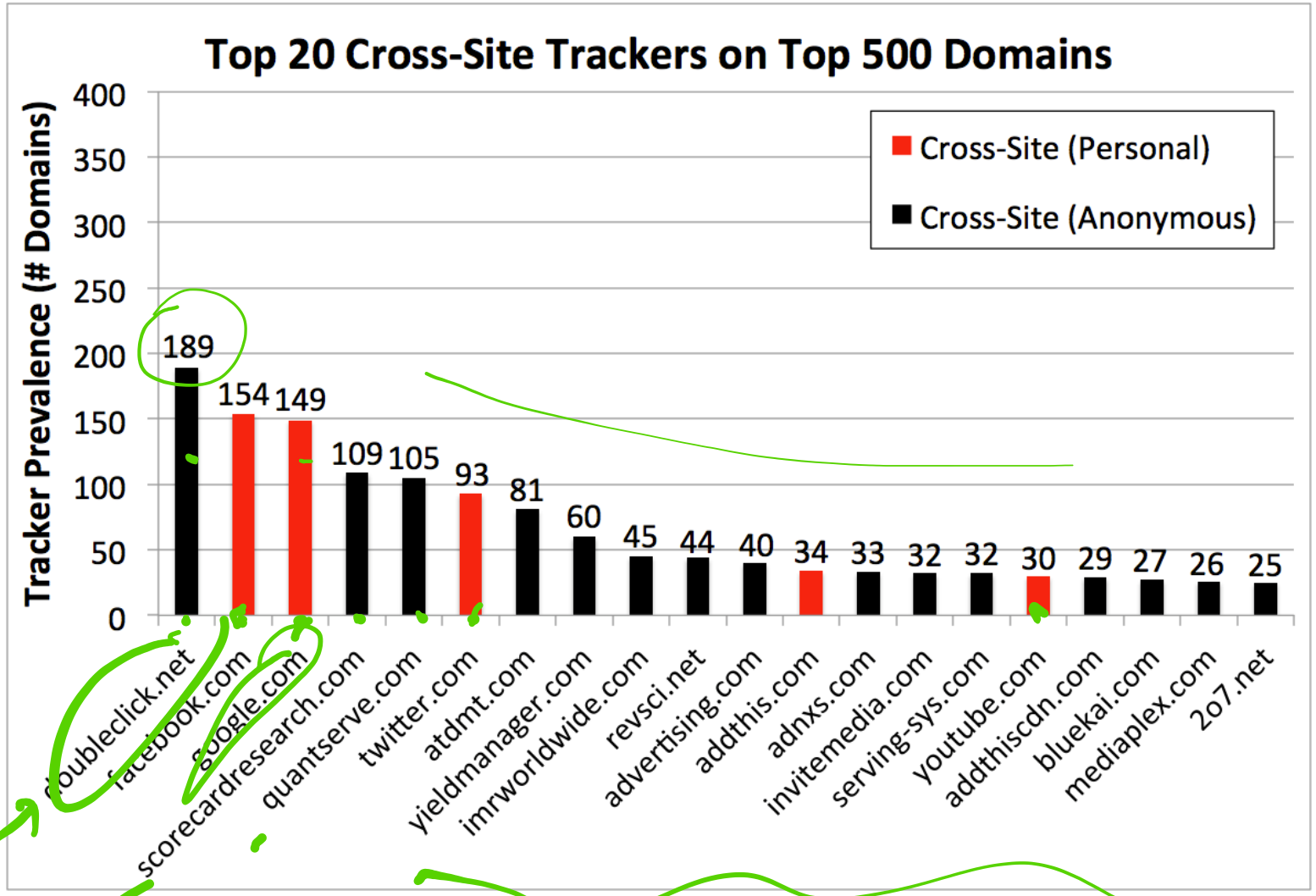


457 domains (91%) embed at least one tracker.
(97% of those include at least one cross-site tracker.)

50% of domains embed between 4 and 5 trackers.

One domain includes 43 trackers.

Who/what are the top trackers? (2011)



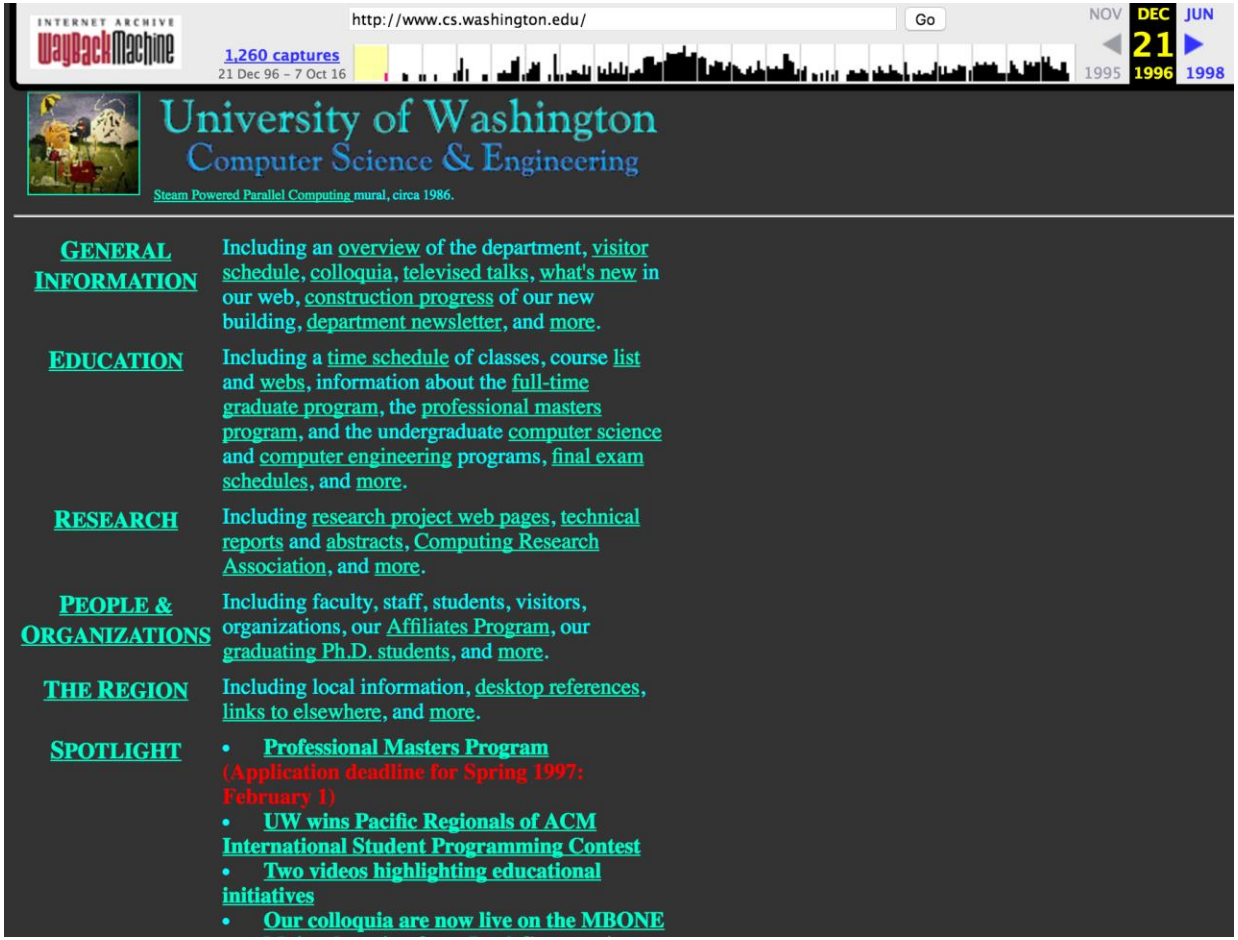
How has this changed over time?

- The web has existed for a while now…
  - What about tracking before 2011? (our first study)
  - What about tracking before 2009? (first academic study)

- Solution: time travel!

archive.org

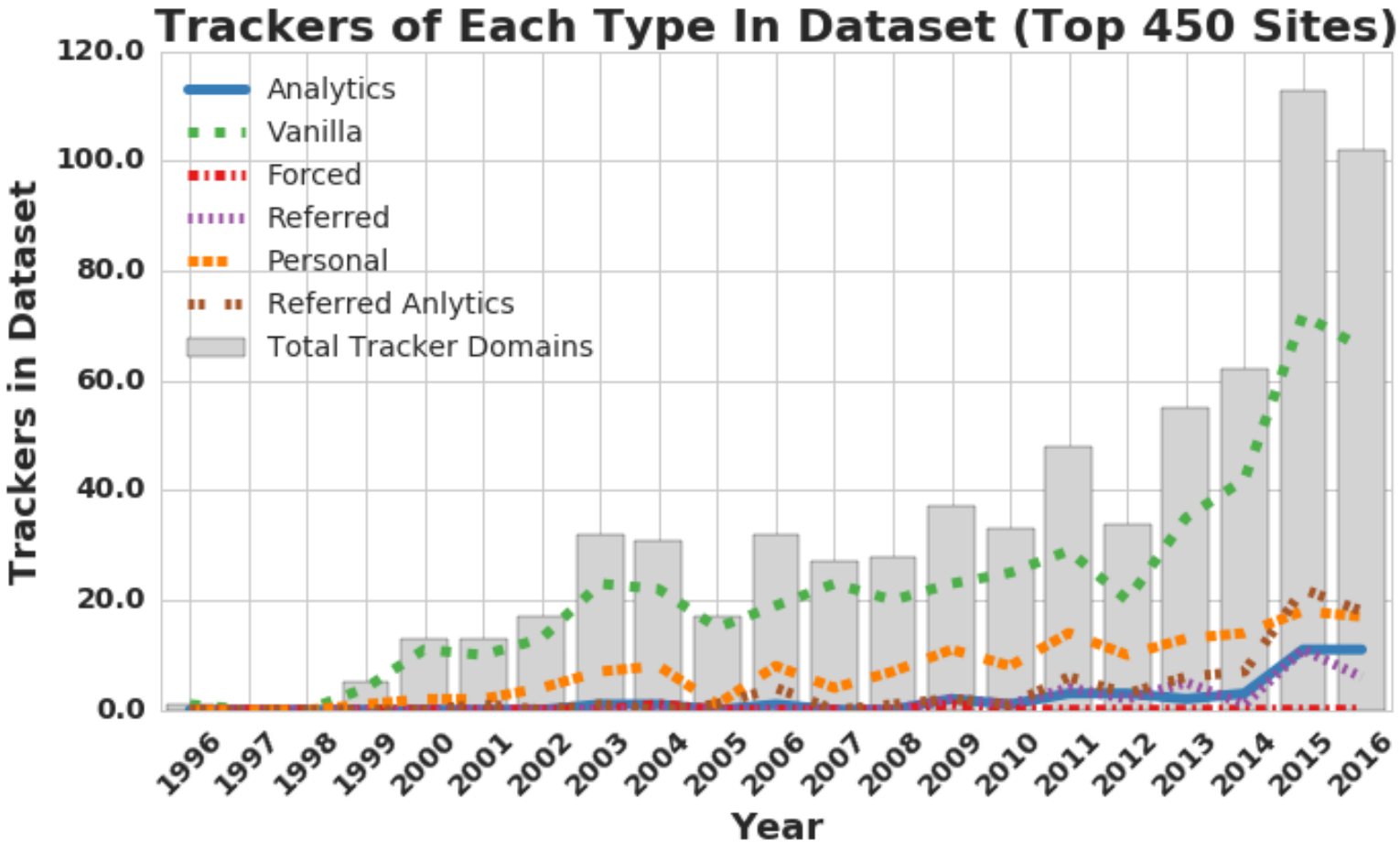
The Wayback Machine to the Rescue



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

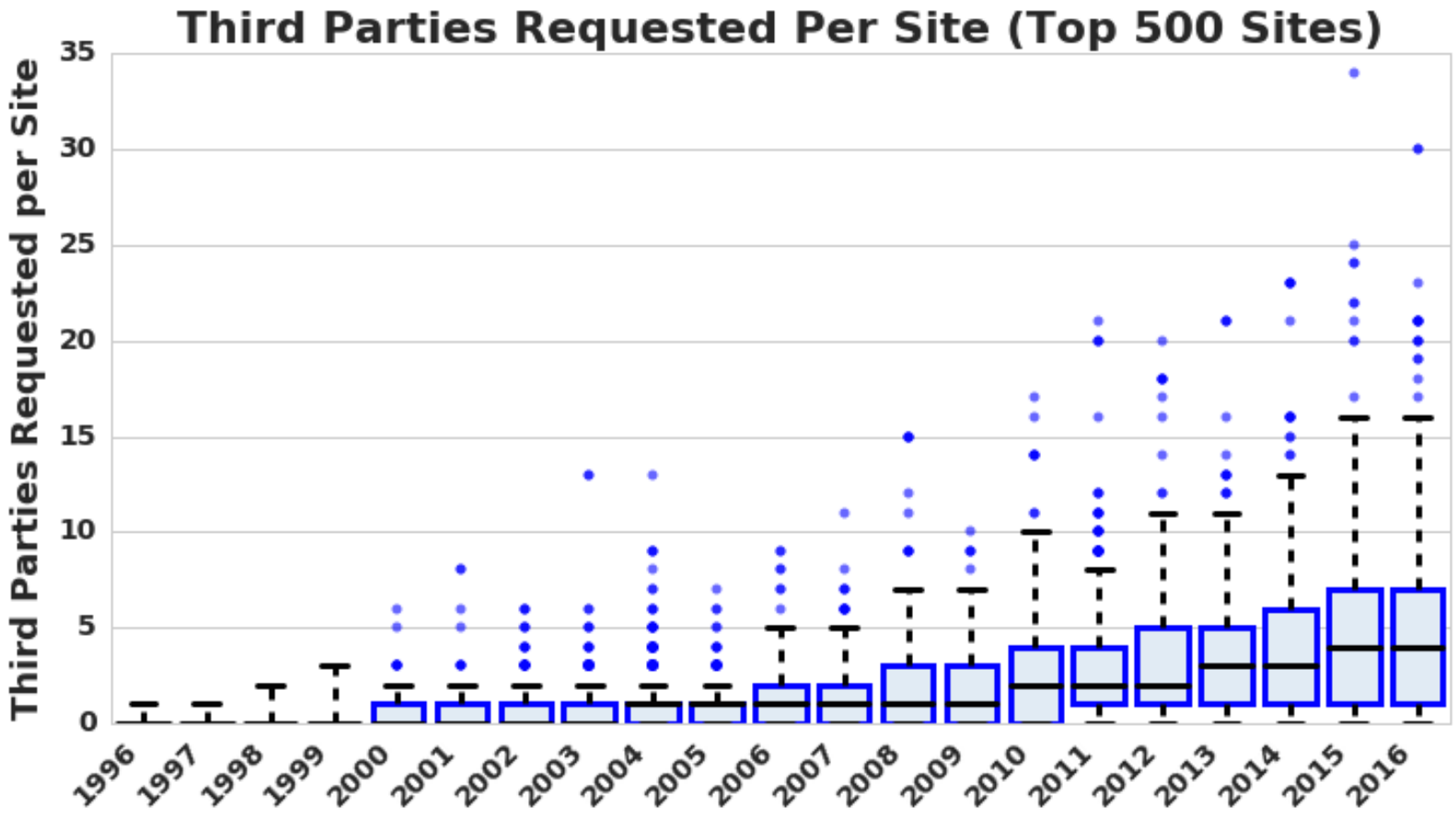
1996-2016: More & More Tracking

- More trackers of more types



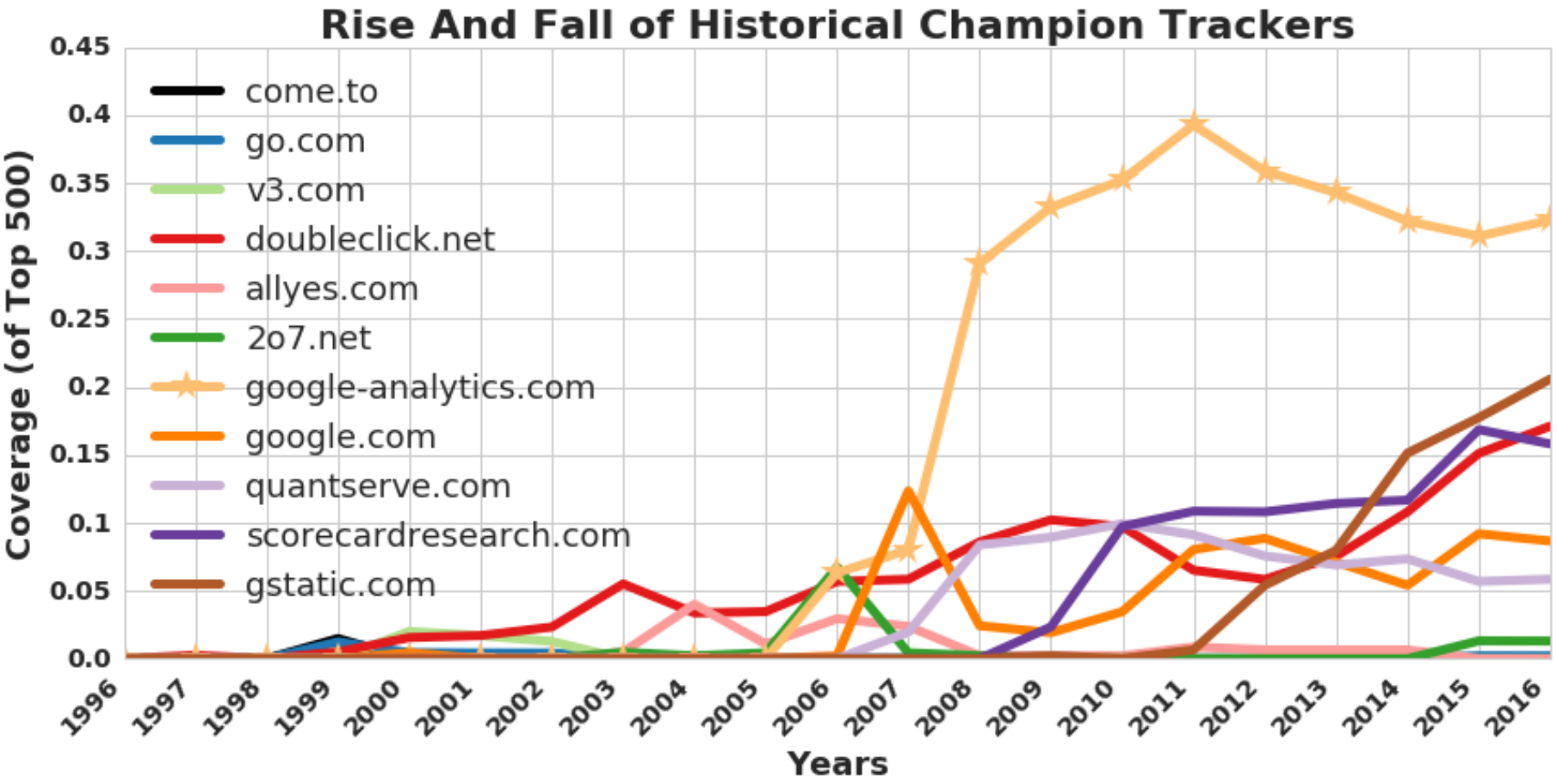
1996-2016: More & More Tracking

- More trackers of more types, more per site



1996-2016: More & More Tracking

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



Outline

1. Understanding web tracking
2. Measuring web tracking
3. Defenses

Defenses to Reduce Tracking

- Do Not Track proposal?

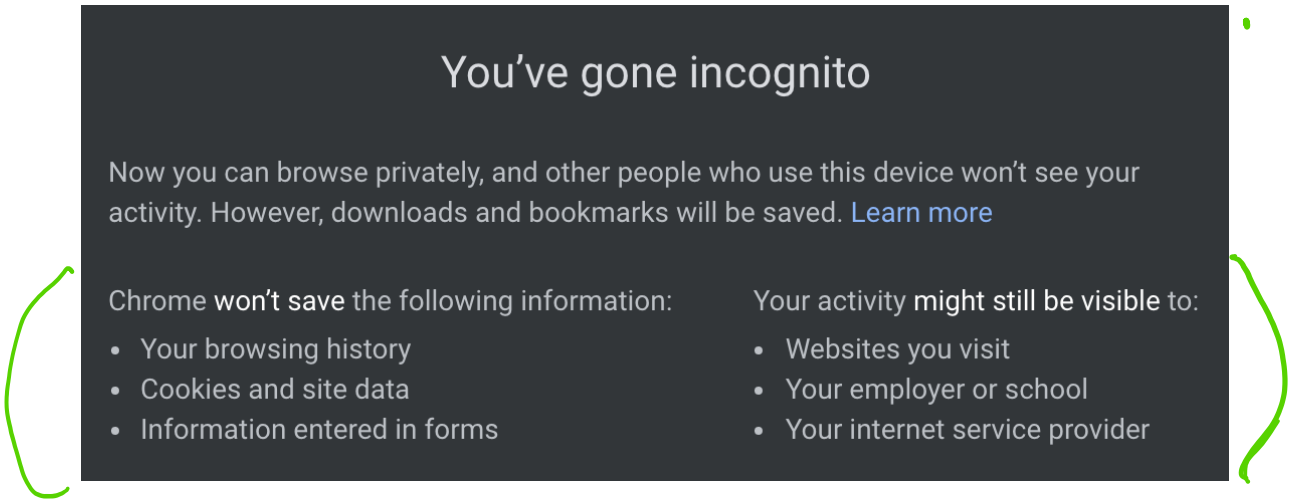
DNT = 1

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

Defenses to Reduce Tracking

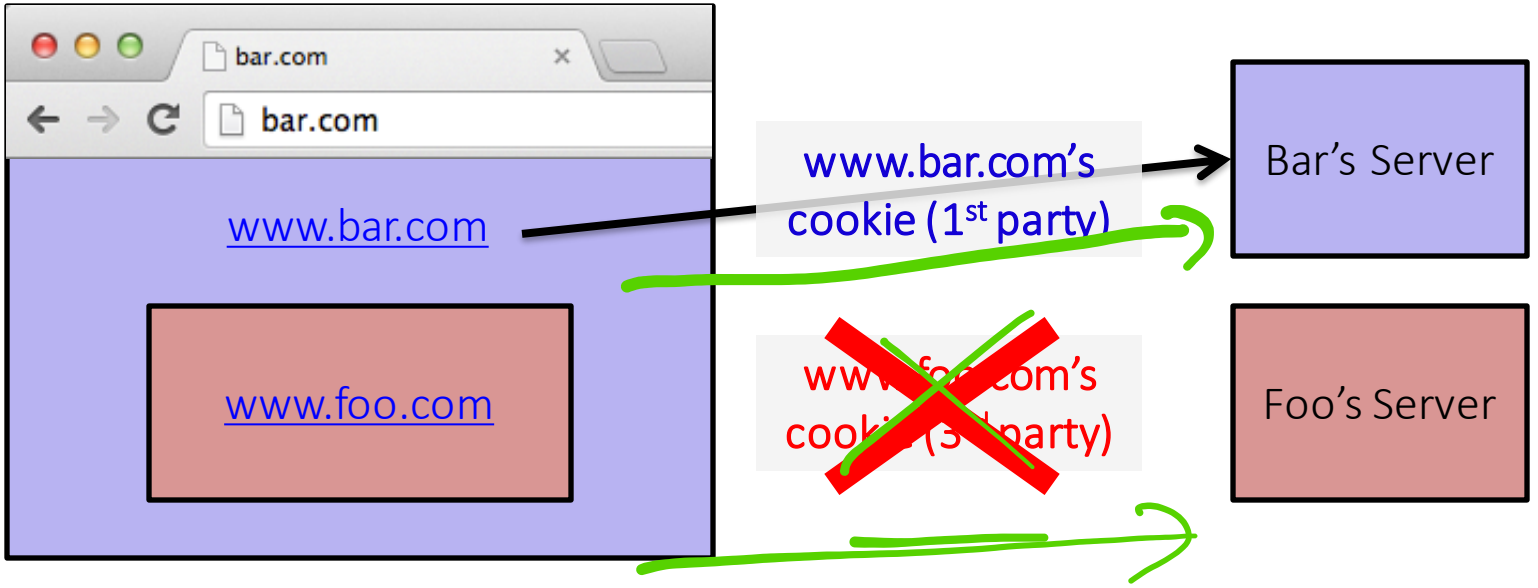
- Do Not Track proposal?
- Private browsing mode?

Private browsing mode protects against local, not network, attackers.



Defenses to Reduce Tracking

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



Quirks of 3rd Party Cookie Blocking

In some browsers, this option means third-party cookies cannot be set, but they CAN be sent.

So if a third-party cookie is somehow set, it can be used.

How to get a cookie set?

One way: be a first party.

Google

etc.

Defenses to Reduce Tracking

- Do Not Track header?
- Private browsing mode?
- Third-party cookie blocking?
- Browser add-ons?

"uses algorithmic methods to decide what is and isn't tracking"

Often rely on blacklists, which may be incomplete.