CSE 484 / CSE M 584: Computer Security and Privacy

Web Security
[Web Privacy]

Spring 2019

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

- Guest lecture on Friday
  - **Emily McReynolds** from Microsoft, on law+policy
- Rest of quarter overview
  - **Final project checkpoint** due Friday (May 17)
  - **Lab 2** due next Friday (May 24)
  - **Homework 3** out soon, due May 31
  - **Final project checkpoint 2** also due May 31
  - **Lab 3** on smart home security coming up
  - **No section in last week; No class on last day**

Last Word on Web App Security…

Storing State in Hidden Forms

- Dansie Shopping Cart (2006)
  - "A premium, comprehensive, Perl shopping cart. Increase your web sales by making it easier for your web store customers to order."

```
<FORM METHOD=POST
 ACTION="http://www.dansie.net/cgi-bin/scripts/cart.pl">

  Black Leather purse with leather straps<

  <INPUT TYPE=HIDDEN NAME=name      VALUE="Black leather purse">
  <INPUT TYPE=HIDDEN NAME=price     VALUE="20.00">
  <INPUT TYPE=HIDDEN NAME=sh        VALUE="1">
  <INPUT TYPE=HIDDEN NAME=img       VALUE="p
  <INPUT TYPE=HIDDEN NAME=custom1   VALUE="B
    with leather straps">

  <INPUT TYPE=SUBMIT NAME="add" VALUE="Put in Shopping Cart">
</FORM>
```

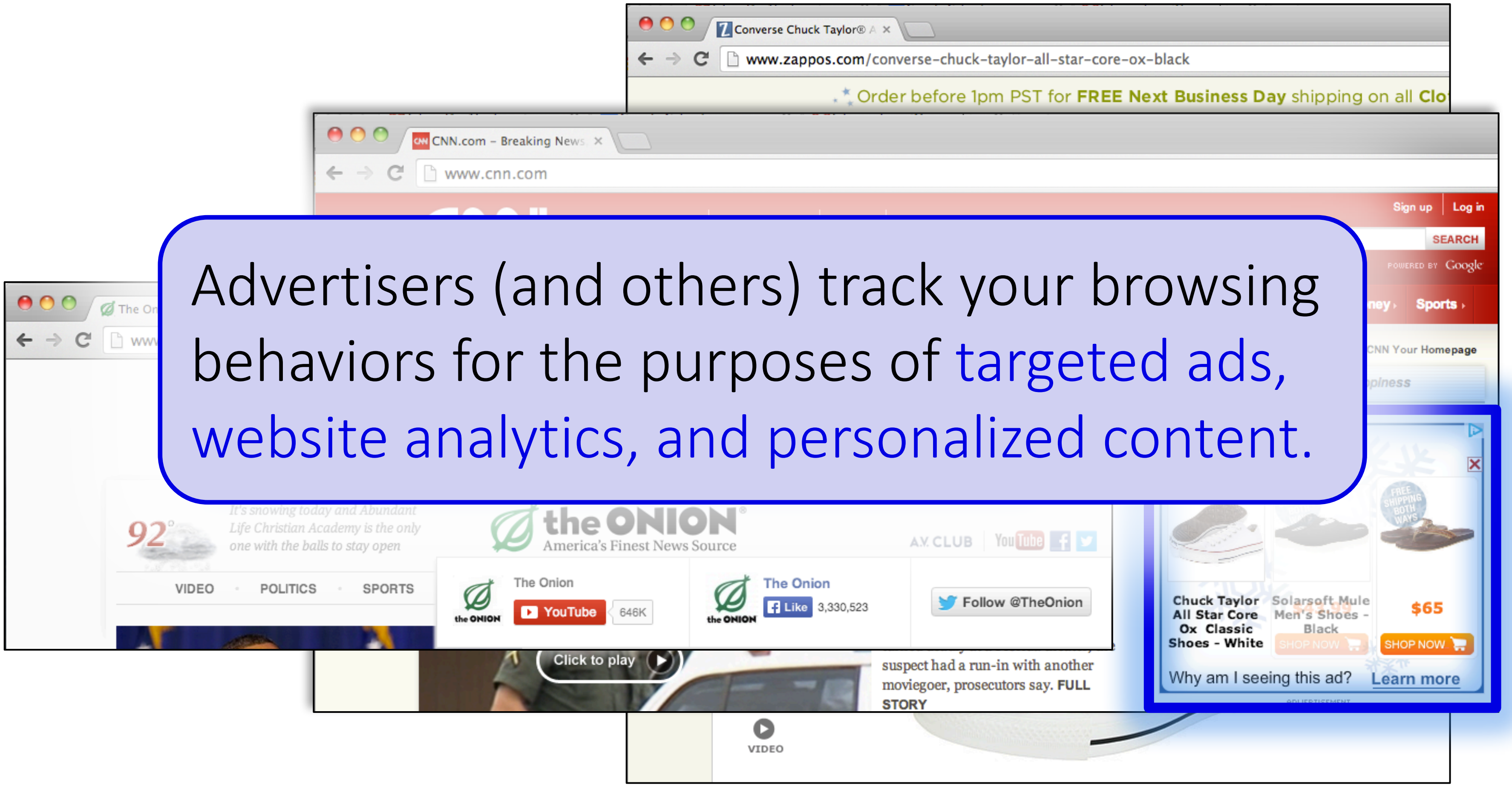
Change this to 2.00

Bargain shopping!

Fix: MAC client-side data, or, more likely, keep on server.

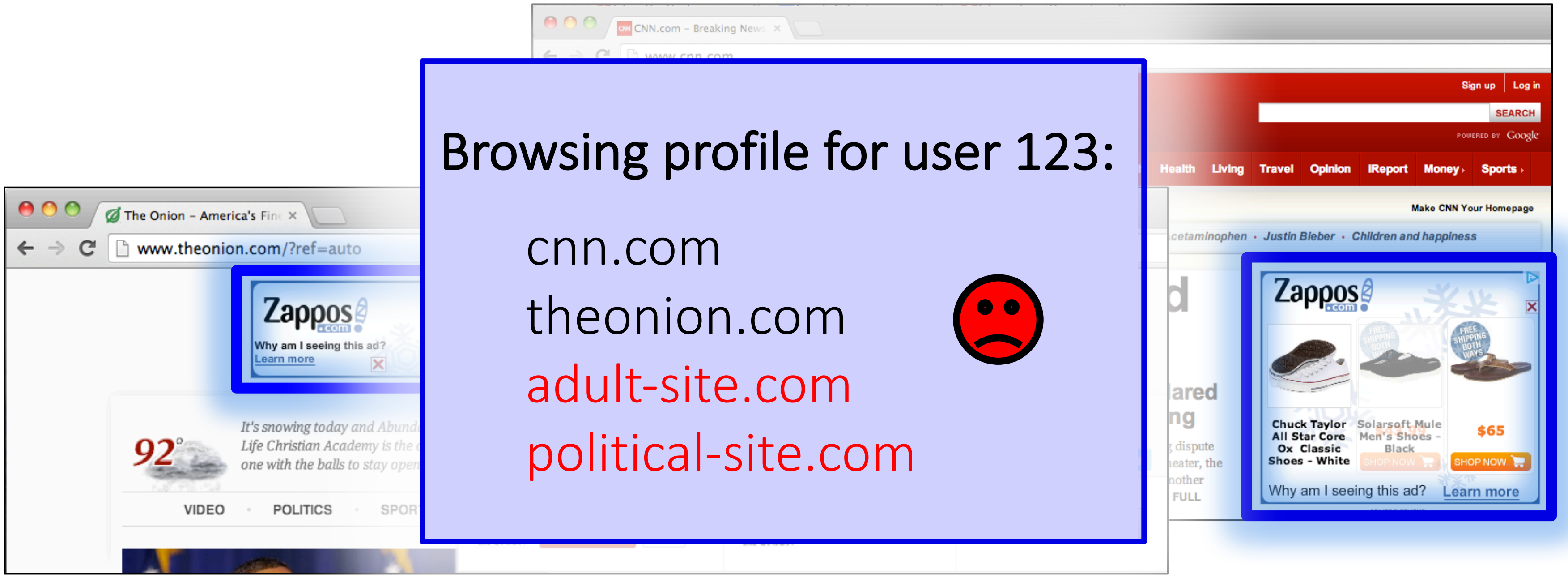
Web Privacy

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 On
92°
It's snowing today and Abundant Life Christian Academy is the only one with the balls to stay open
VIDEO
POLITICS
SPORTS
the ONION
America's Finest News Source
A.V. CLUB
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
Chuck Taylor All Star Core Ox Classic Shoes - White
Solarsoft Mule Men's Shoes - Black
$65
SHOP NOW
FREE SHIPPING BOTH WAYS
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

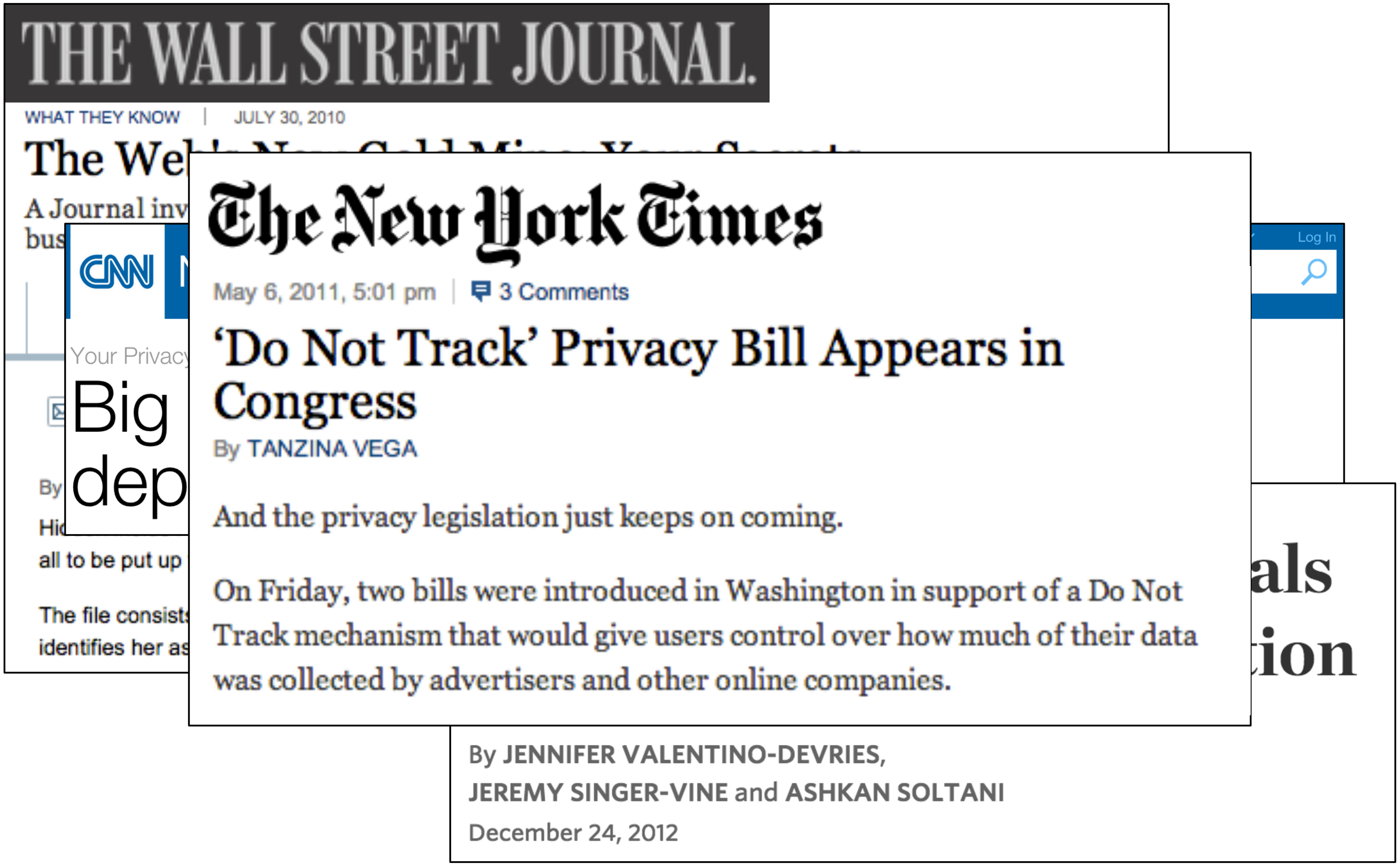
theonion.com

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.

Concerns About Privacy



THE WALL STREET JOURNAL.

WHAT THEY KNOW | JULY 30, 2010

The We

A Journal inv
bus

By

Hi
all to be put up

The file consists
identifies her as

Your Privacy

Big
dep

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.

Log In

als
ion

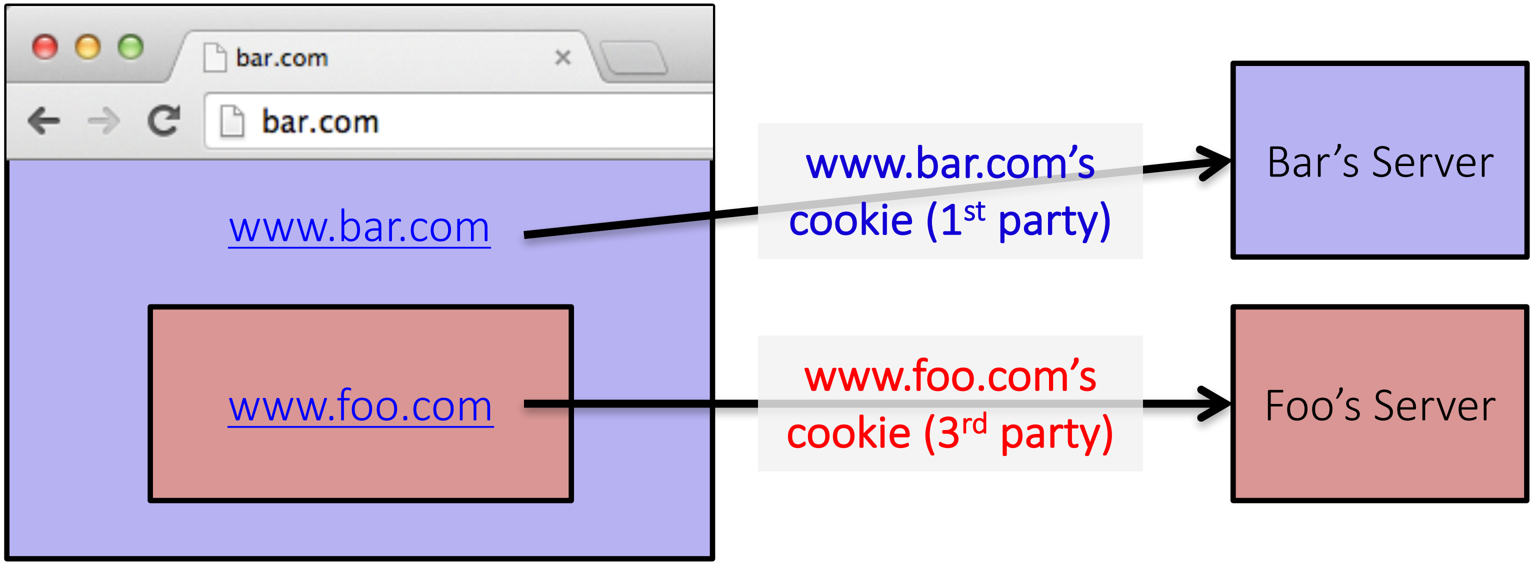
By JENNIFER VALENTINO-DEVRIES,
JEREMY SINGER-VINE and ASHKAN SOLTANI
December 24, 2012

Outline

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

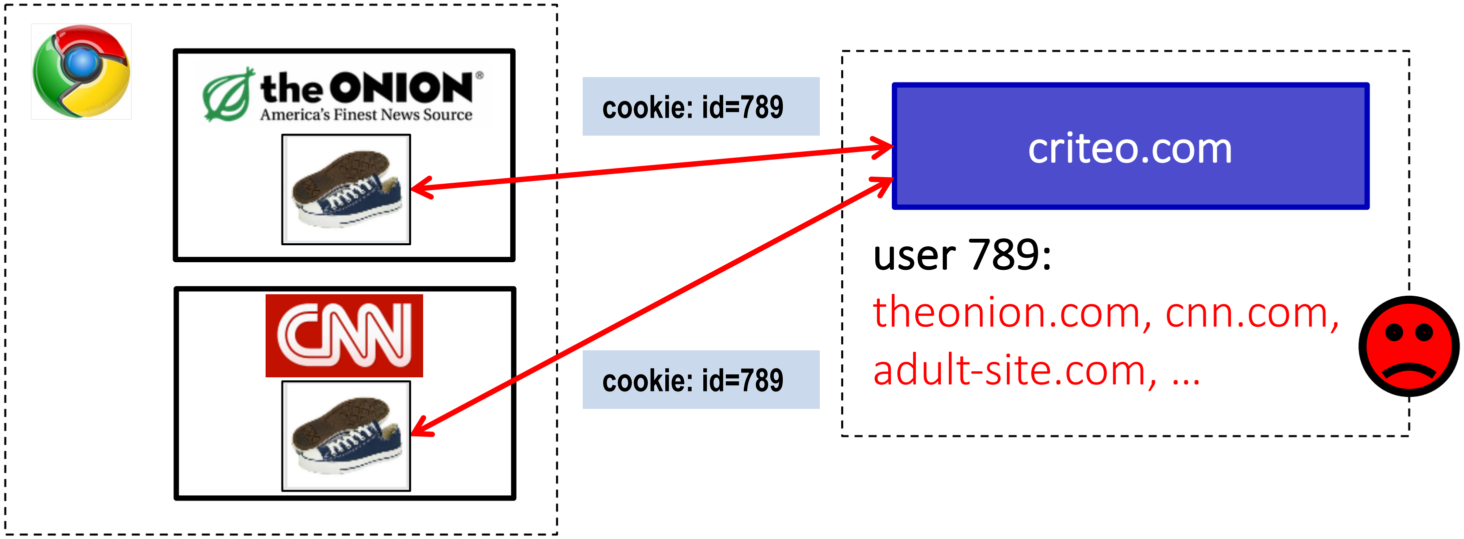
Recall: First and Third Parties

- 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

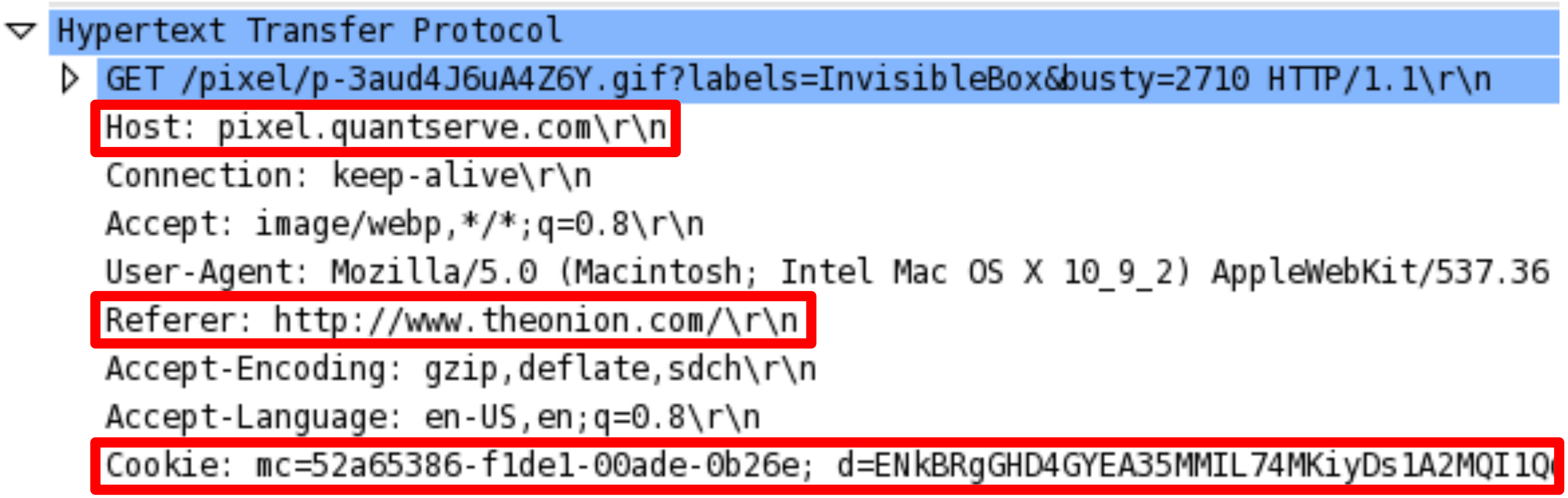
Anonymous Tracking

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

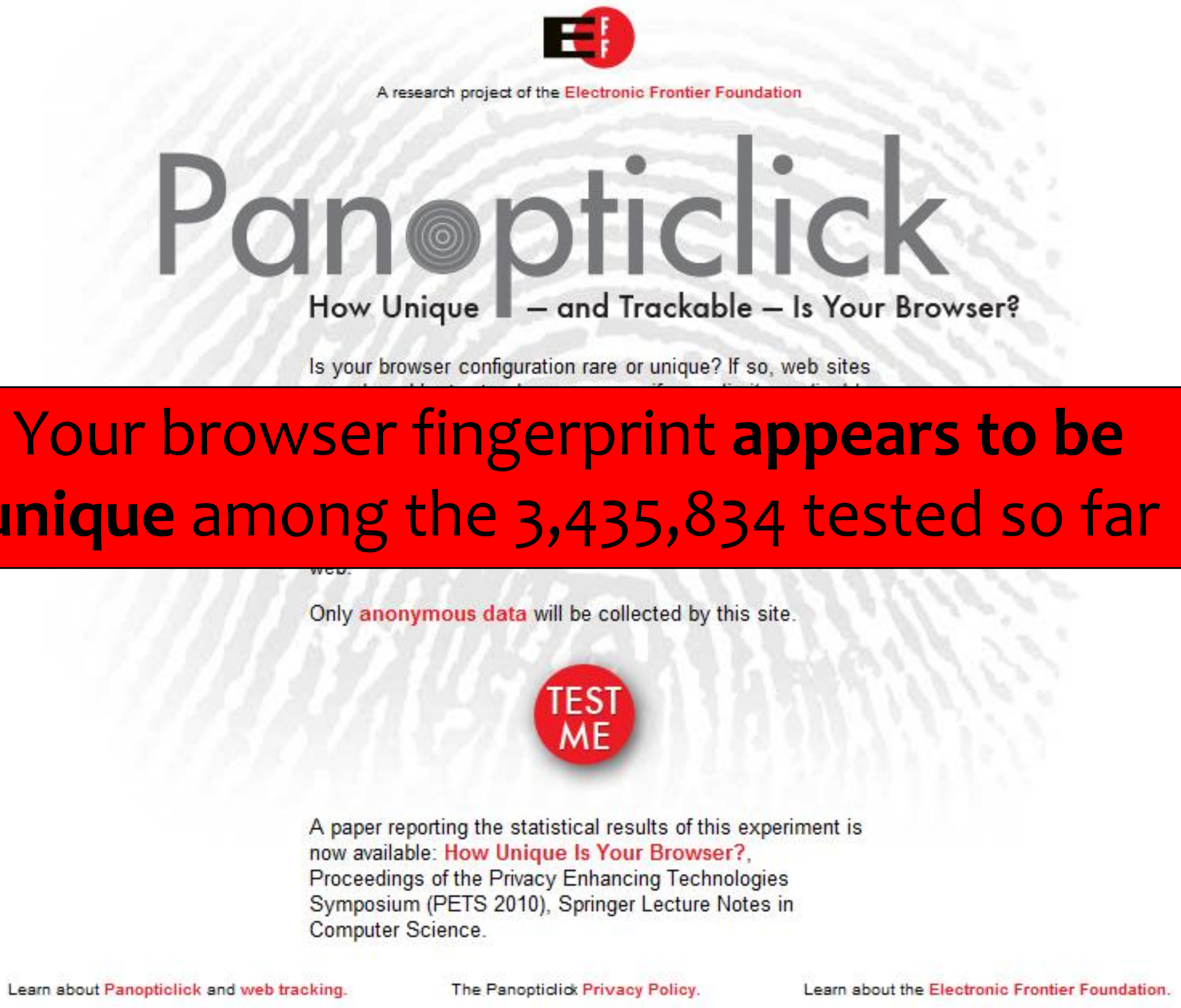
- Flash cookies
- Silverlight storage
- TLS session ID & resume
- Browsing history
- window.name
- HTTP STS
- DNS cache

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

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!)

Your browser fingerprint **appears to be unique** among the 3,435,834 tested so far



A research project of the Electronic Frontier Foundation

Panopticlick

How Unique — and Trackable — Is Your Browser?

Is your browser configuration rare or unique? If so, web sites

web.

Only anonymous data will be collected by this site.

A paper reporting the statistical results of this experiment is now available: How Unique Is Your Browser?, Proceedings of the Privacy Enhancing Technologies Symposium (PETS 2010), Springer Lecture Notes in Computer Science.

Learn about Panopticlick and web tracking.

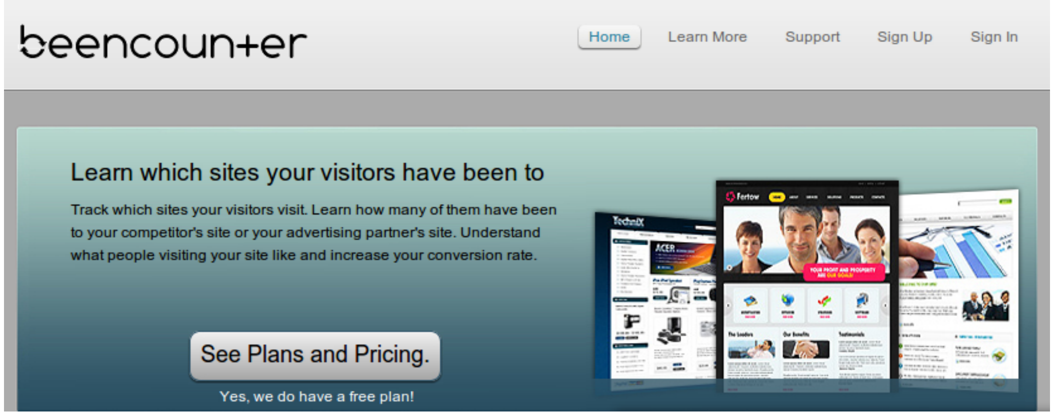
The Panopticlick Privacy Policy.

Learn about the Electronic Frontier Foundation.

History Sniffing

How can a webpage figure out which sites you visited previously?

- Color of links
  - CSS :visited property
  - getComputedStyle()
- Cached Web content timing
- DNS timing

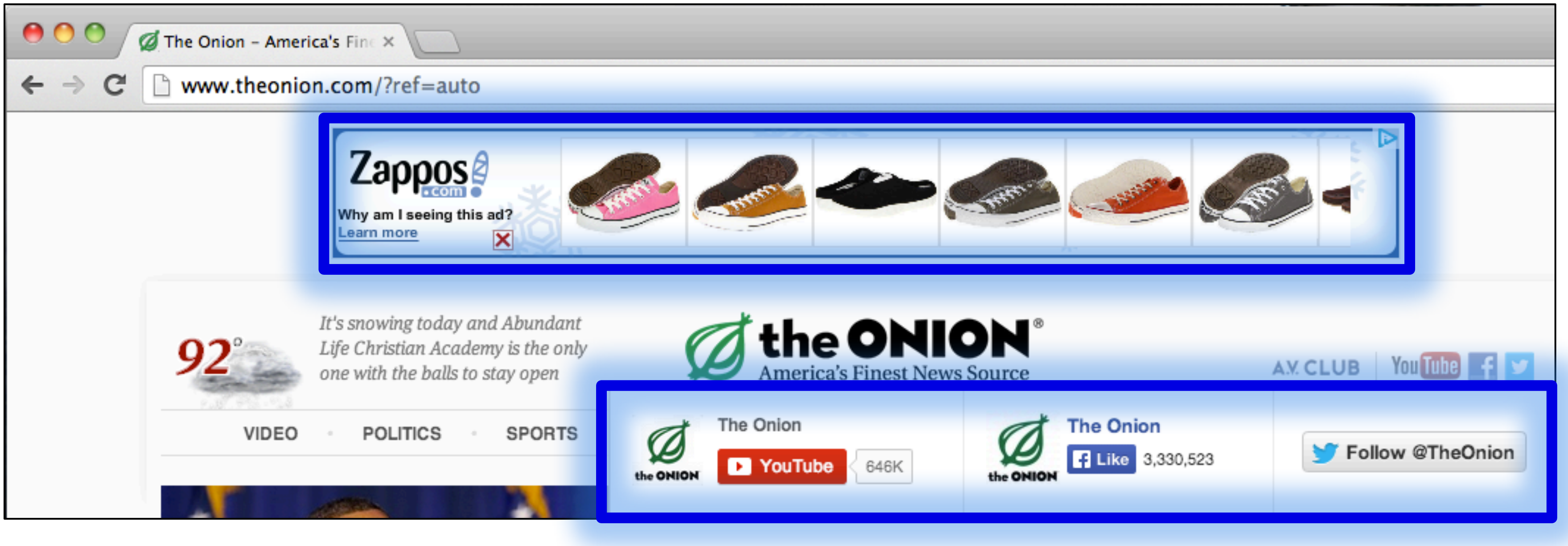


Learn which sites your visitors have been to

Track which sites your visitors visit. Learn how many of them have been to your competitor's site or your advertising partner's site. Understand what people visiting your site like and increase your conversion rate.

Yes, we do have a free plan!

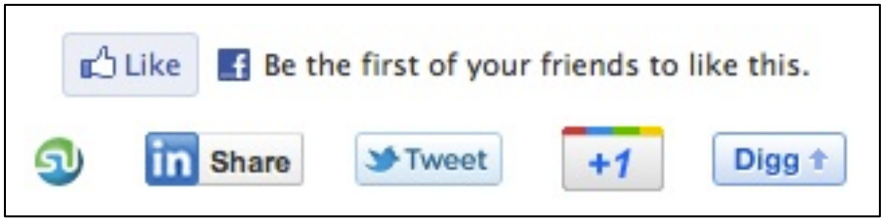
Other Trackers?



www.theonion.com/?ref=auto

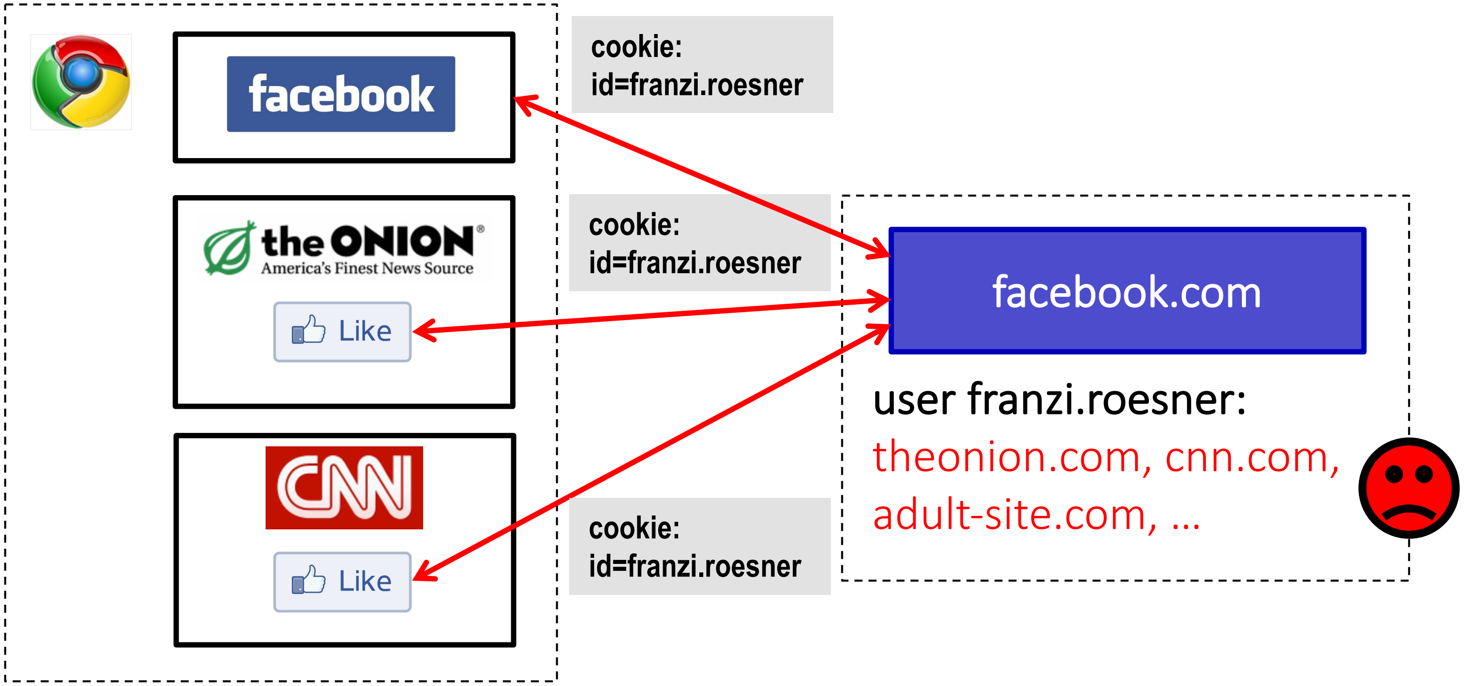
It's snowing today and Abundant Life Christian Academy is the only one with the balls to stay open

“Personal” Trackers



Be the first of your friends to like this.

Personal Tracking



- 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

[NSDI ‘12]

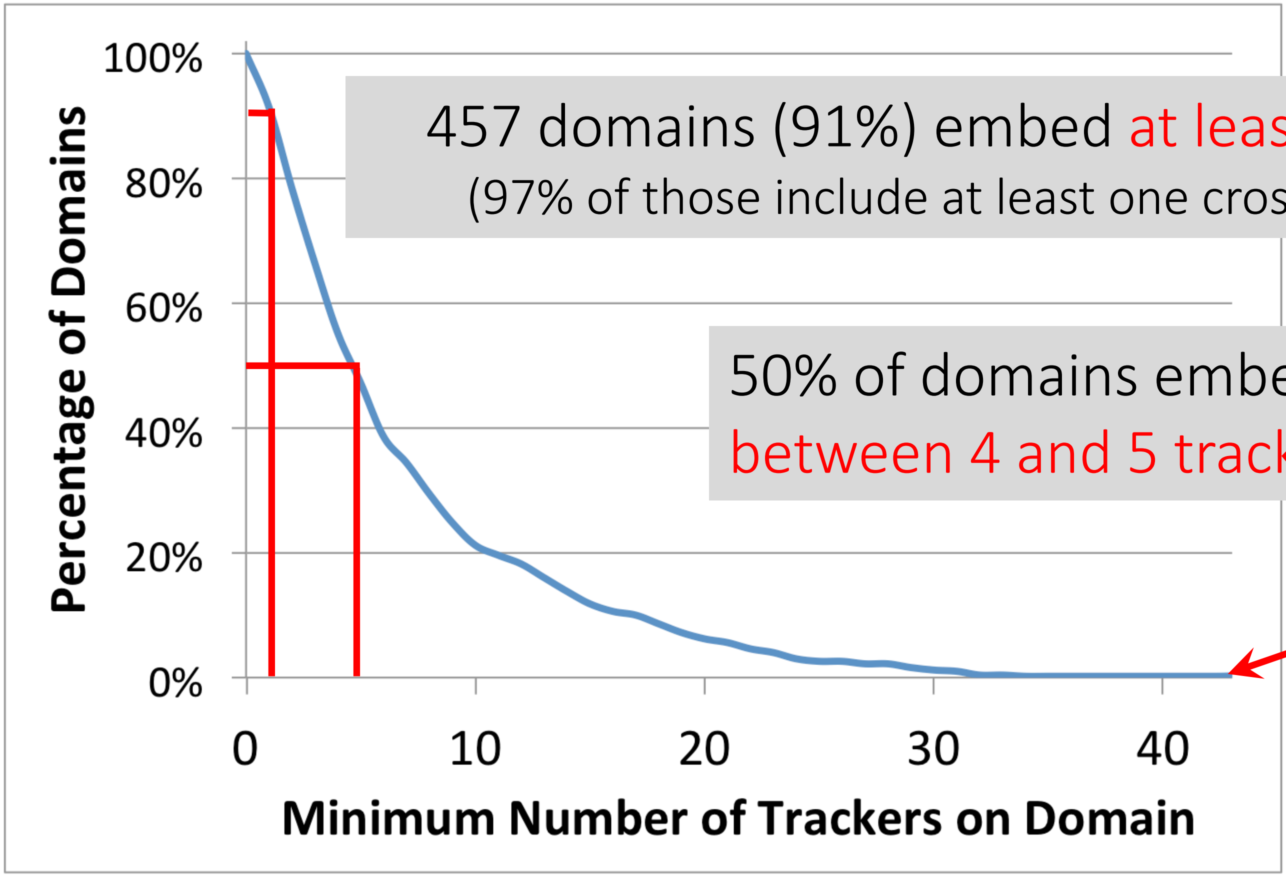
Measurement Study

- **Questions:**
  - How prevalent is tracking (of different types)?
  - How much of a user’s browsing history is captured?
  - How effective are defenses?
- **Approach:** Build tool to automatically crawl web, detect and categorize trackers based on our taxonomy.

Longitudinal studies since then: tracking has increased and become more complex.

How prevalent is tracking? (2011)

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

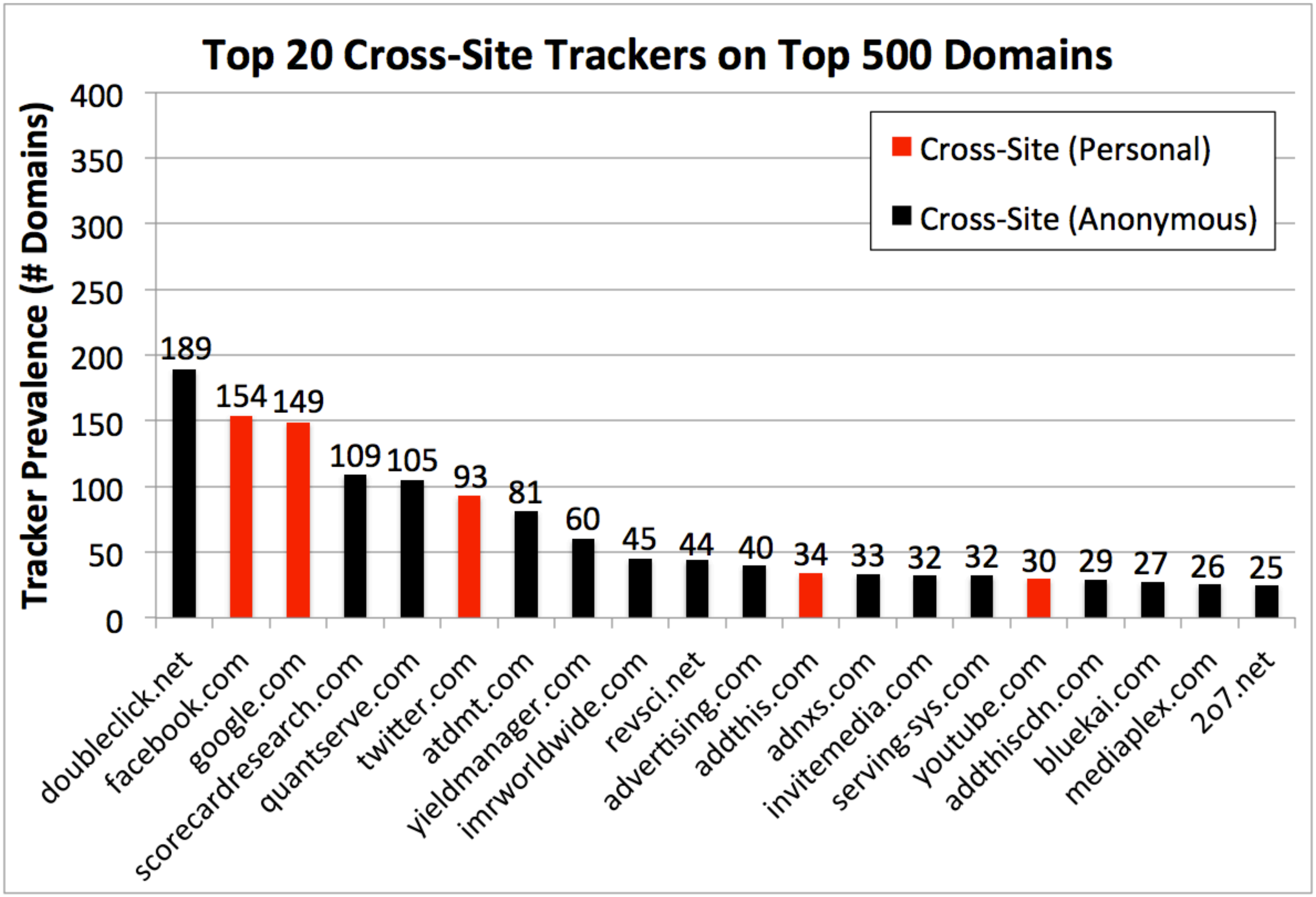


457 domains (91%) embed at least one tracker.
(97% of those include at least one cross-site tracker.)

50% of domains embed between 4 and 5 trackers.

One domain includes 43 trackers.

Who/what are the top trackers? (2011)



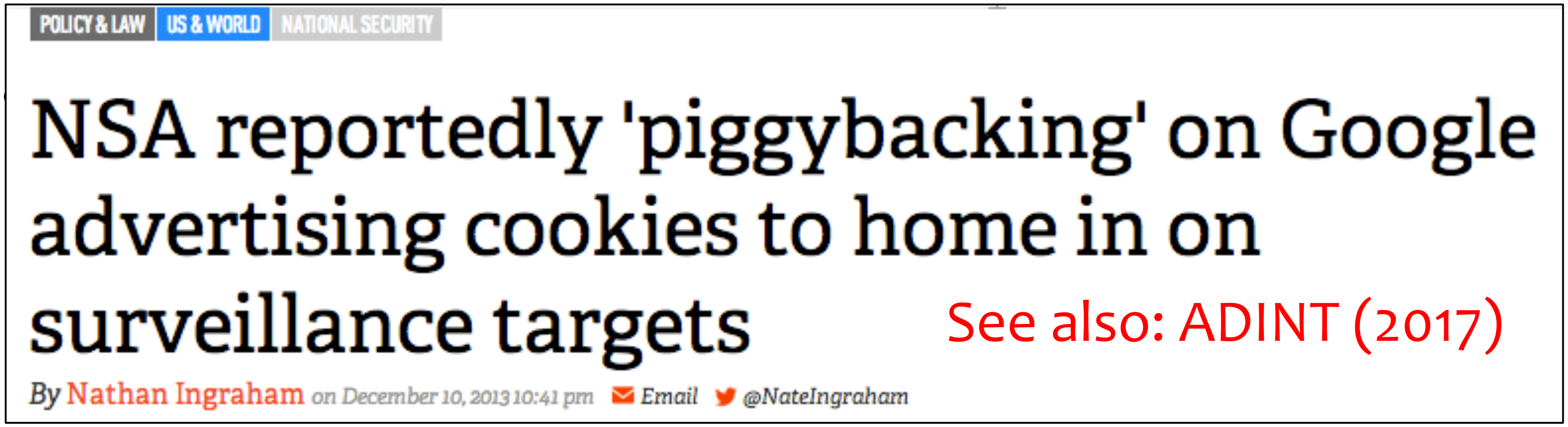
How are users affected?

- Question: How much of a real user's browsing history can top trackers capture?
- Measurement challenges:
  - Privacy concerns.
  - Users may not browse realistically while monitored.
- Insight: AOL search logs (released in 2006) represent real user behaviors.

How are users affected?

- Idea: Use AOL search logs to create 30 hypothetical browsing histories.
  - 300 unique queries per user → top search hits.
- Trackers can capture a large fraction:
  - Doubleclick: Avg 39% (Max 66%)
  - Facebook: Avg 23% (Max 45%)
  - Google: Avg 21% (Max 61%)

How are users affected?



POLICY & LAW US & WORLD NATIONAL SECURITY

NSA reportedly 'piggybacking' on Google advertising cookies to home in on surveillance targets

By Nathan Ingraham on December 10, 2013 10:41 pm Email @NateIngraham

See also: ADINT (2017)

- Trackers can capture a large fraction:
  - Doubleclick: Avg 39% (Max 66%)
  - Facebook: Avg 23% (Max 45%)
  - Google: Avg 21% (Max 61%)

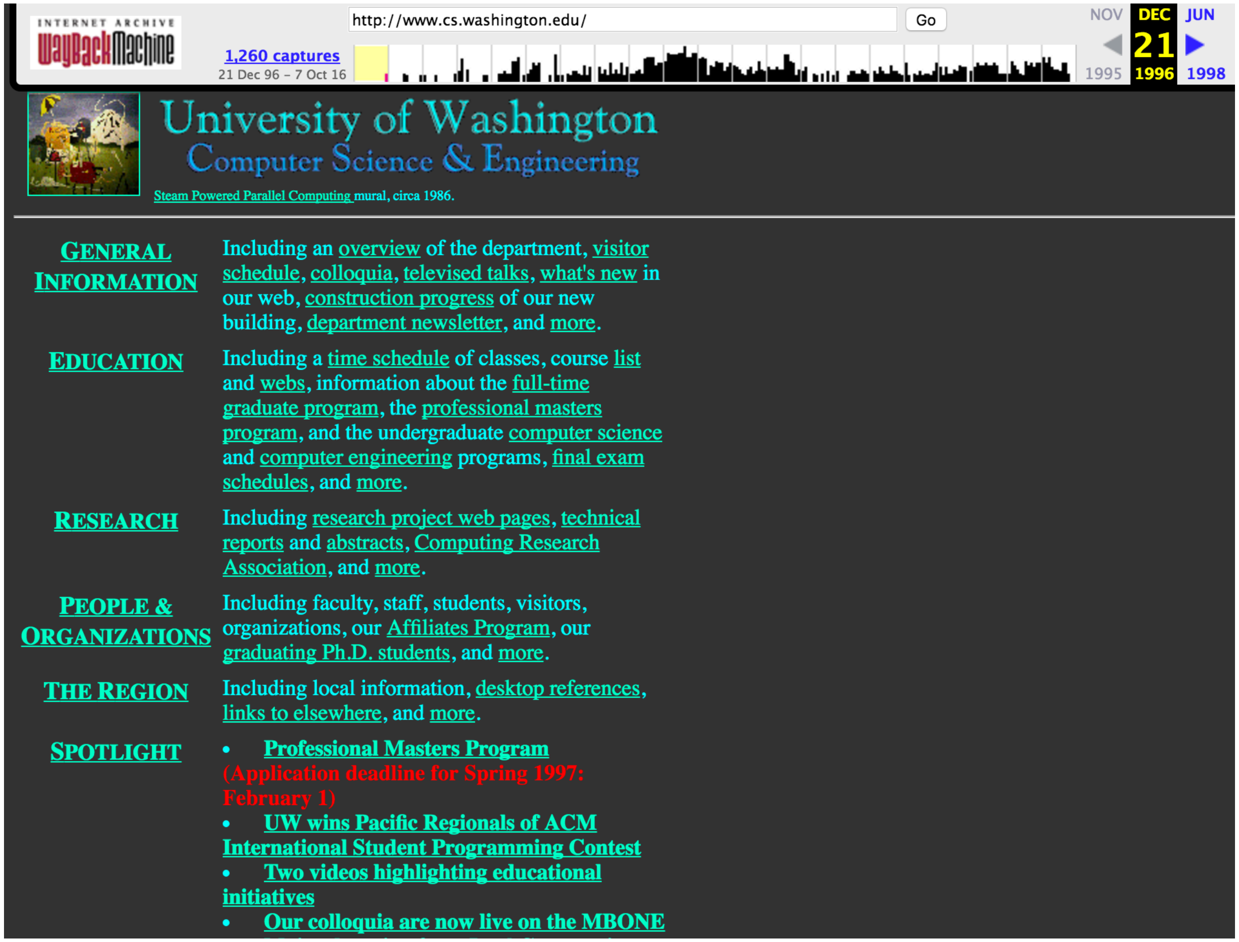
How has this changed over time?

- 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!

  [USENIX Security '16]

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.

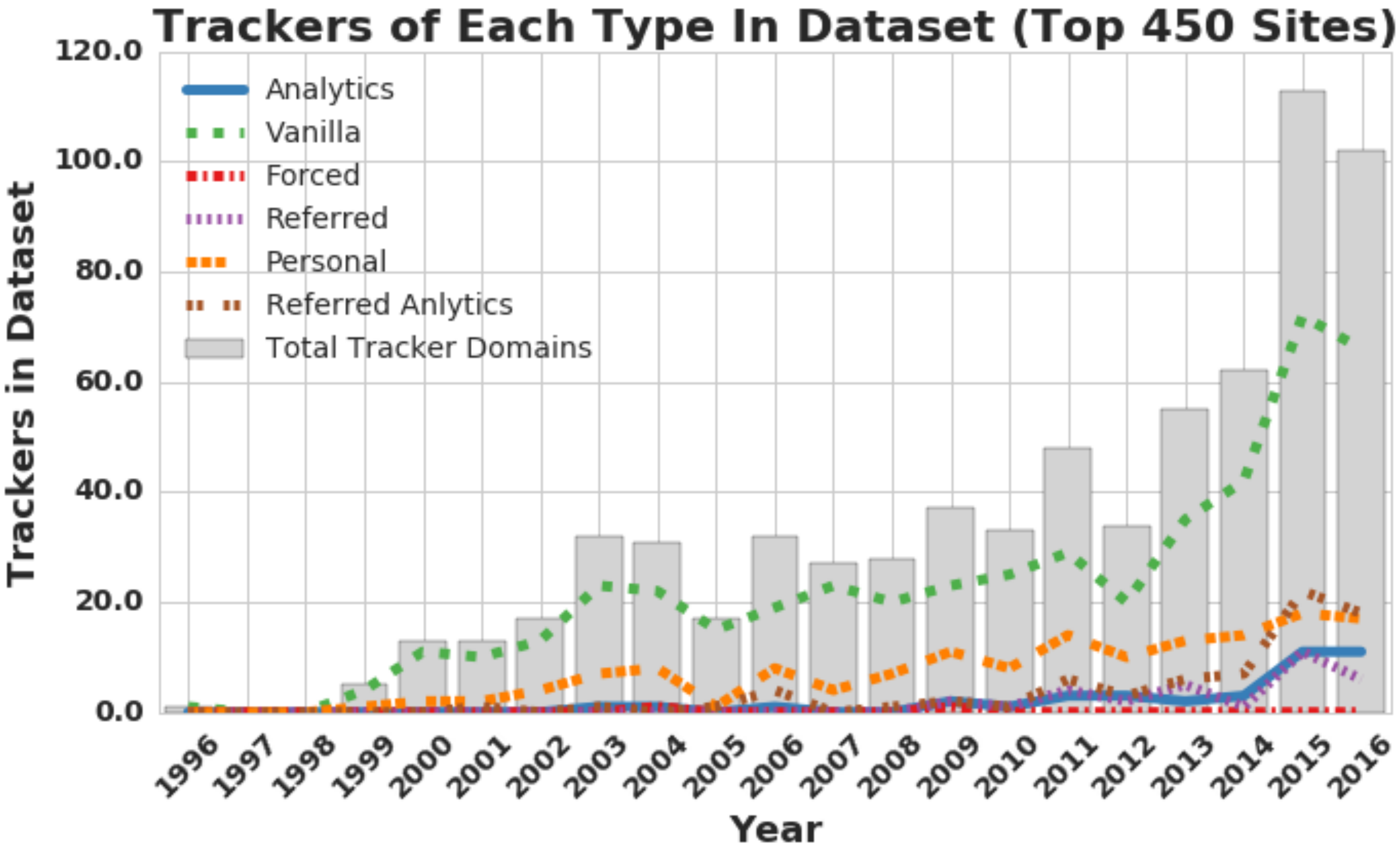
SPOTLIGHT

- **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

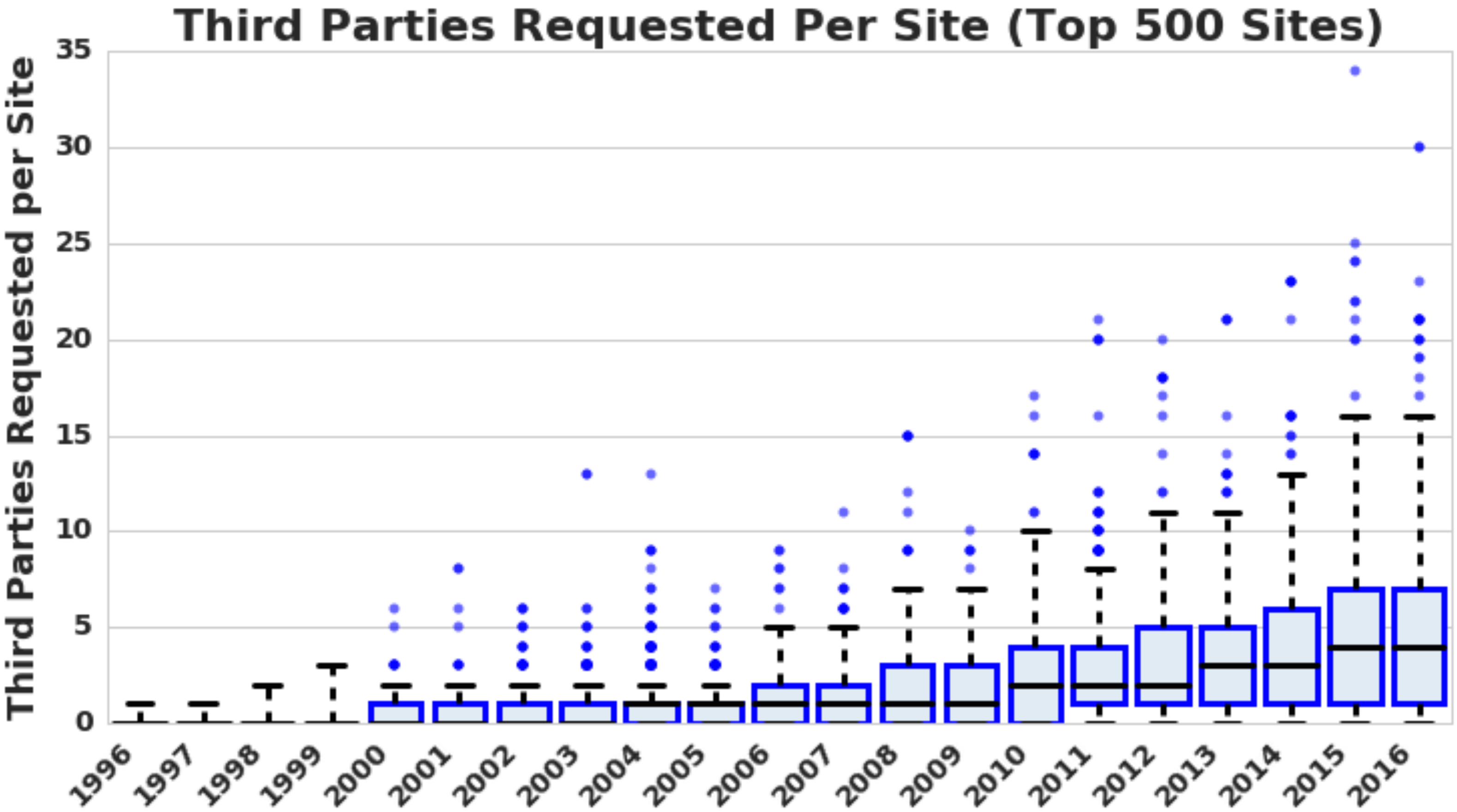
1996-2016: More & More Tracking

- More trackers of more types



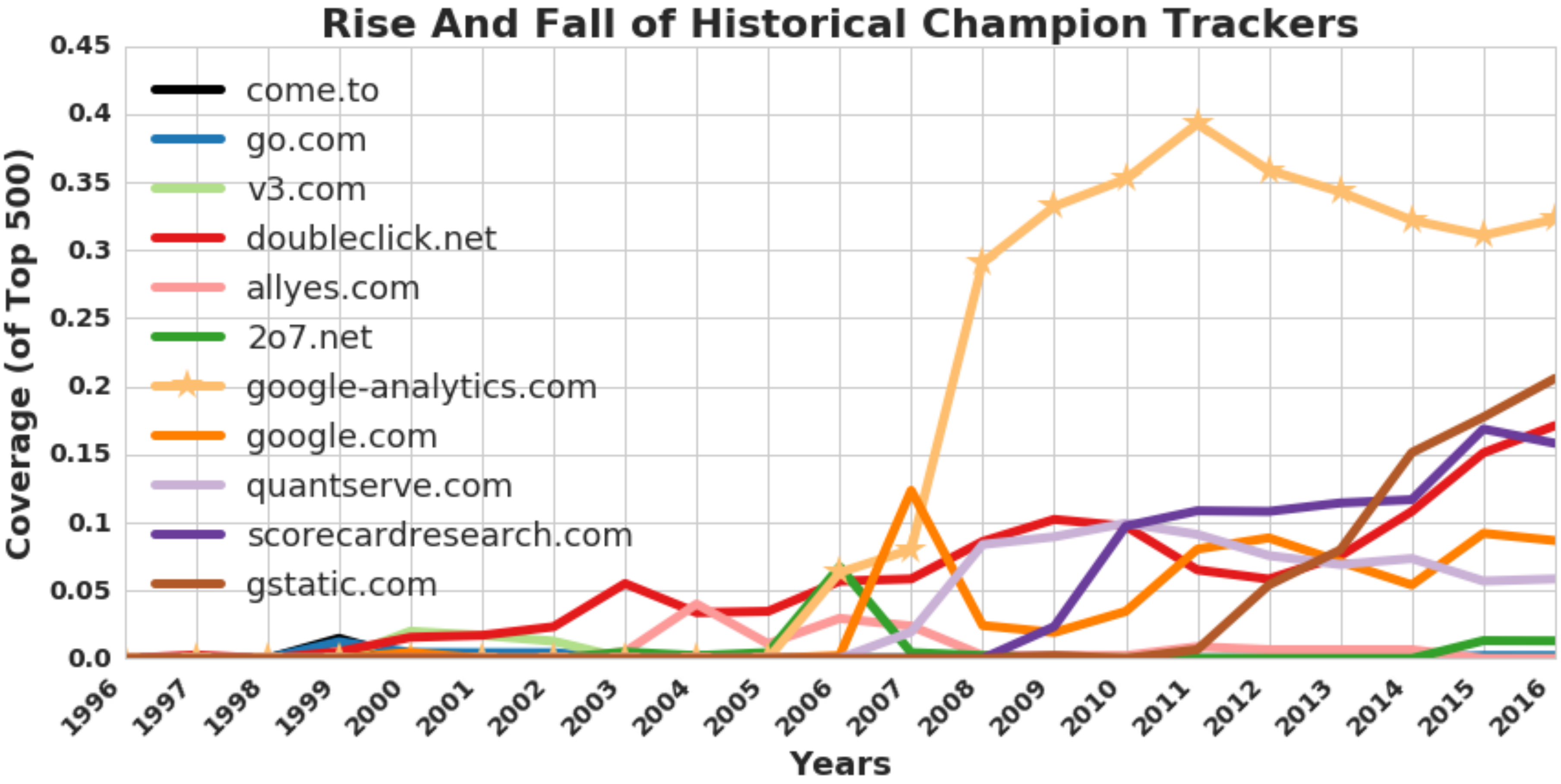
1996-2016: More & More Tracking

- More trackers of more types, more per site



1996-2016: More & More Tracking

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

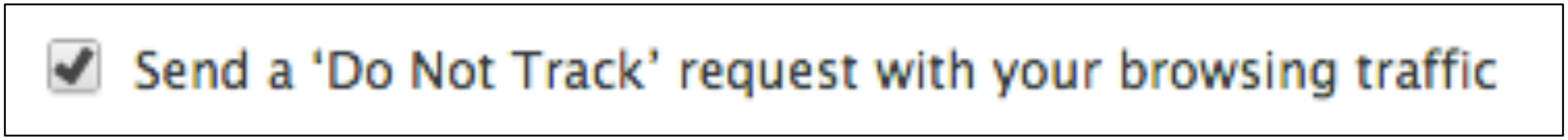


Outline

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

Defenses to Reduce Tracking

- Do Not Track proposal?



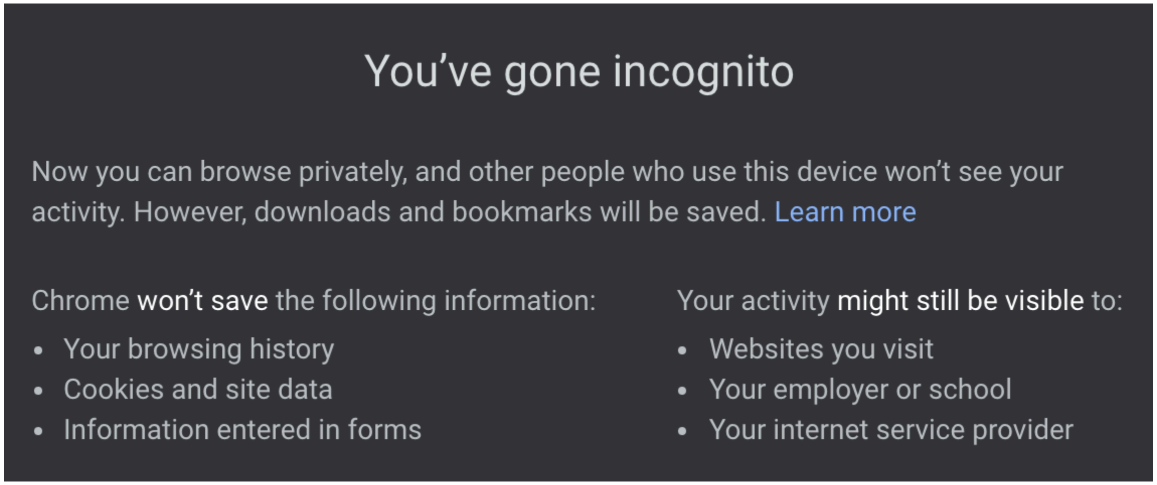
☑ Send a 'Do Not Track' request with your browsing traffic

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:

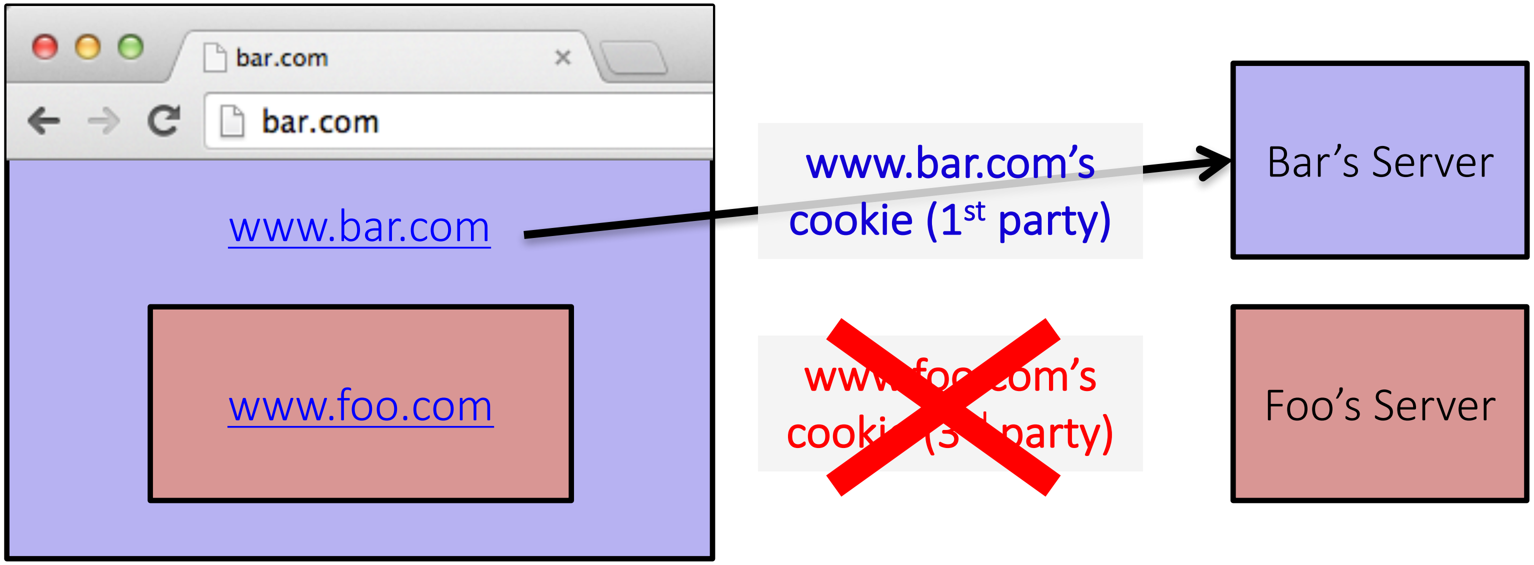
- Your browsing history
- Cookies and site data
- Information entered in forms

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

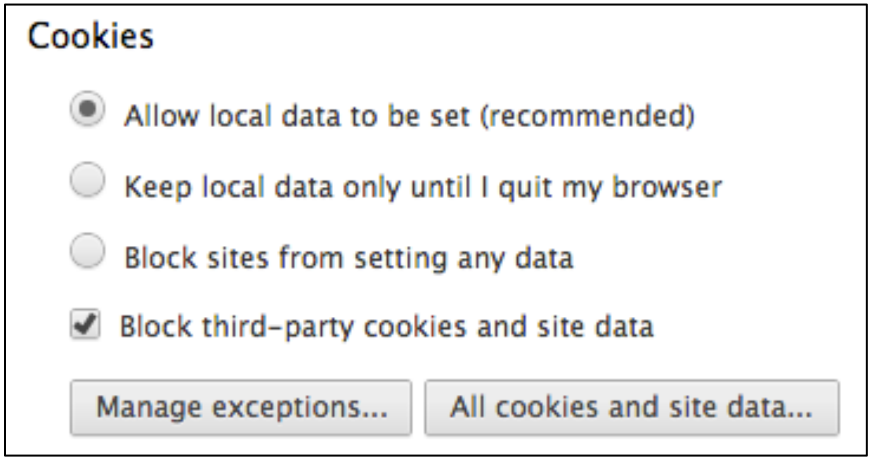
- Websites you visit
- Your employer or school
- Your internet service provider

Defenses to Reduce Tracking

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


bar.com
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

Quirks of 3rd Party Cookie Blocking



Cookies

● Allow local data to be set (recommended)

○ Keep local data only until I quit my browser

○ Block sites from setting any data

☑ Block third-party cookies and site data

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.

etc.

Defenses to Reduce Tracking

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

Ghostery

Lightbeam
for Firefox

Often rely on blacklists, which may be incomplete.

Privacy Badger
A PROJECT OF THE ELECTRONIC FRONTIER FOUNDATION
BETA

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

uBlock Origin