

CSE 484 / CSE M 584: Computer Security and Privacy

Web Security

[Web Application Security, Web Privacy]

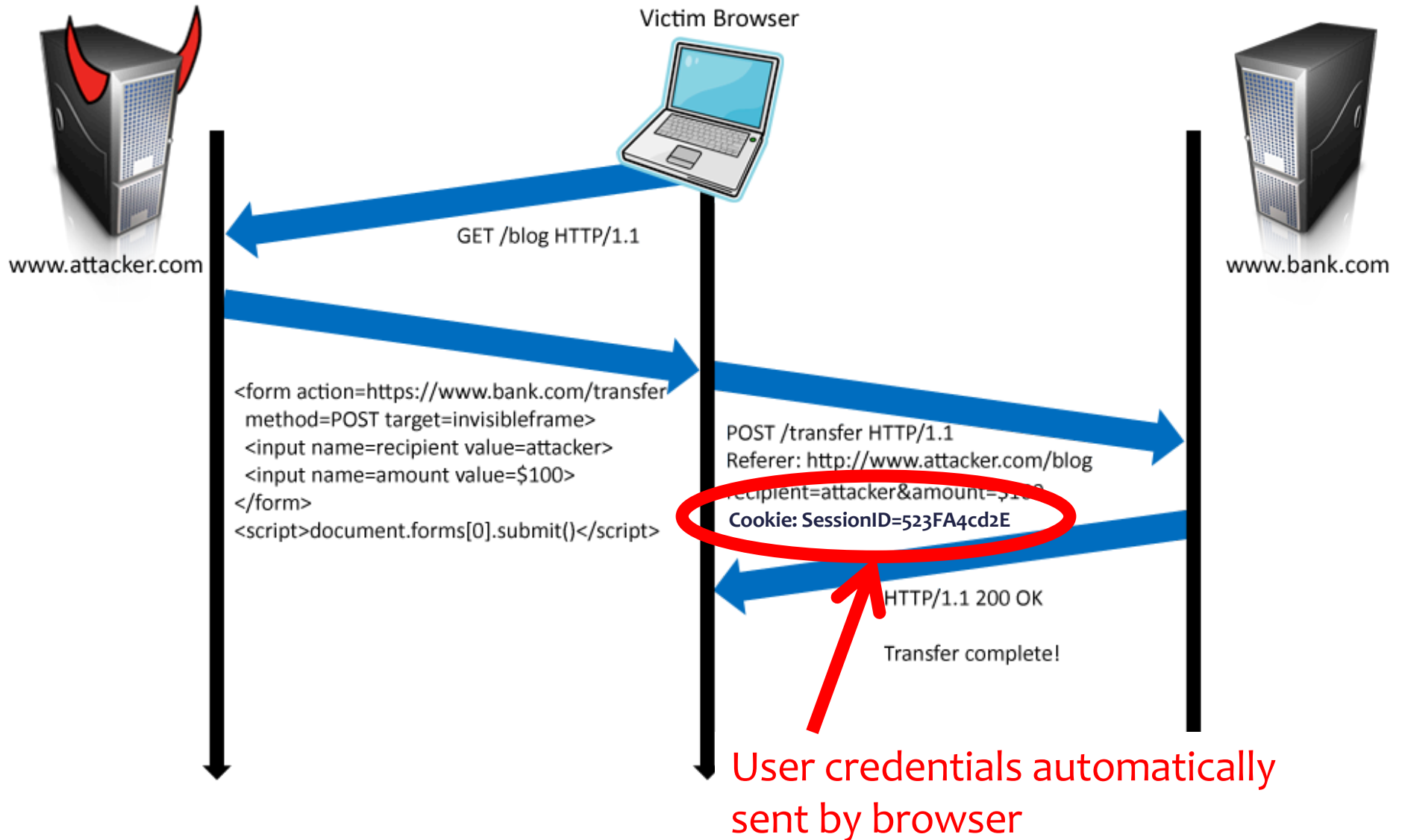
Spring 2020

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 ...

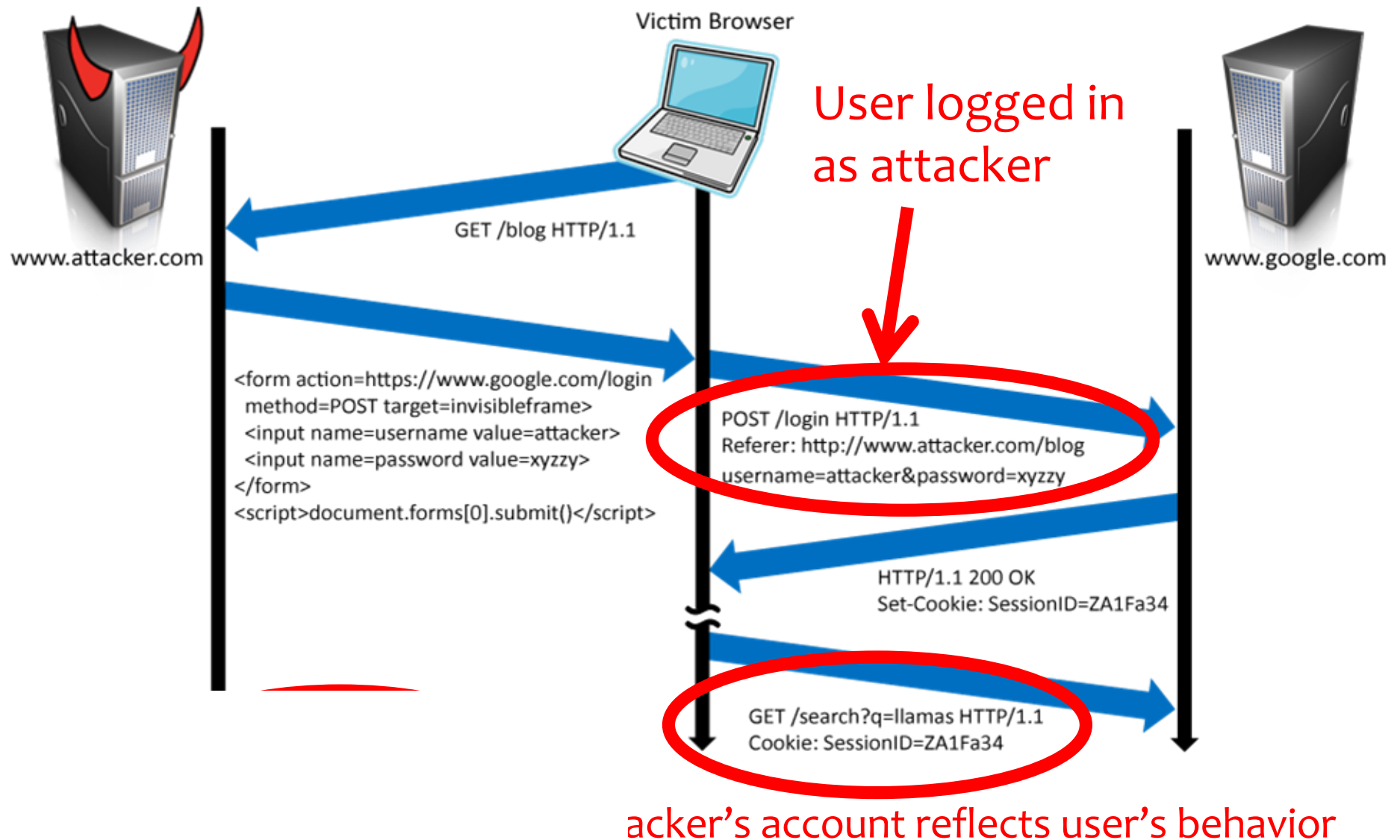
XSRF Recap



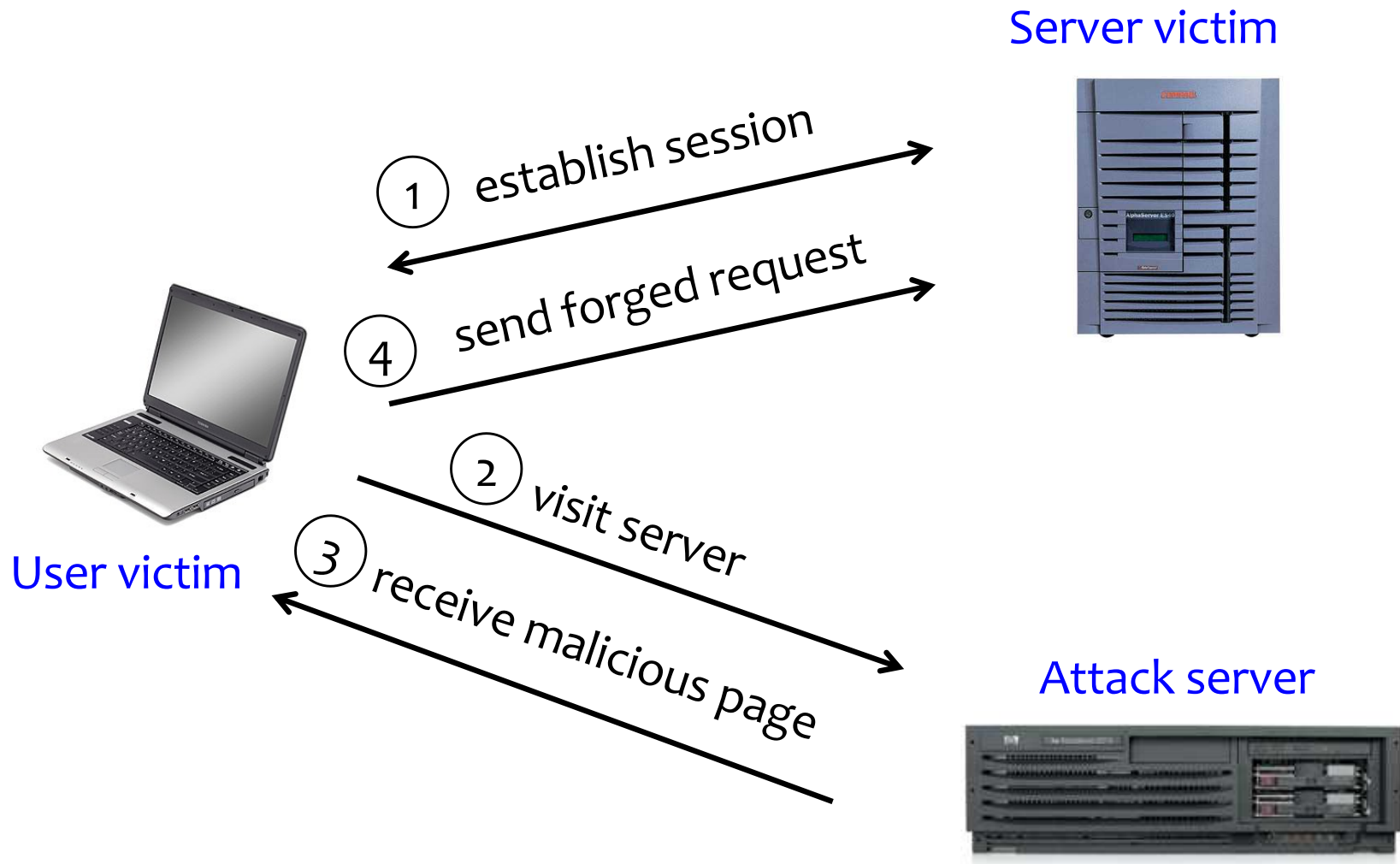
Impact

- Hijack any ongoing session (if no protection)
 - Netflix: change account settings, Gmail: steal contacts, Amazon: one-click purchase
- Reprogram the user's home router
- Login to the *attacker's* account

Login XSRF: Attacker logs you in as them!



XSRF (aka CSRF): Summary



Q: how long do you stay logged on to Gmail? Financial sites?

XSRF Defenses

- Secret validation token



```
<input type=hidden value=23a3af01b>
```

- Referer validation



```
Referer:  
http://www.facebook.com/home.php
```

Add Secret Token to Forms

```
<input type=hidden value=23a3af01b>
```

- “Synchronizer Token Pattern”
- Include a **secret challenge token** as a hidden input in forms
 - Token often based on user’s session ID
 - Server must verify correctness of token before executing sensitive operations
- Why does this work?
 - **Same-origin policy**: attacker can’t read token out of legitimate forms loaded in user’s browser, so can’t create fake forms with correct token

Referer Validation

Facebook Login

For your security, never enter your Facebook password on sites not located on Facebook.com.

Email:

Password:

☐ Remember me

[Login](#) or [Sign up for Facebook](#)

[Forgot your password?](#)



Referer:
`http://www.facebook.com/home.php`



Referer:
`http://www.evil.com/attack.html`



Referer:

- **Lenient** referer checking – header is optional
- **Strict** referer checking – header is required

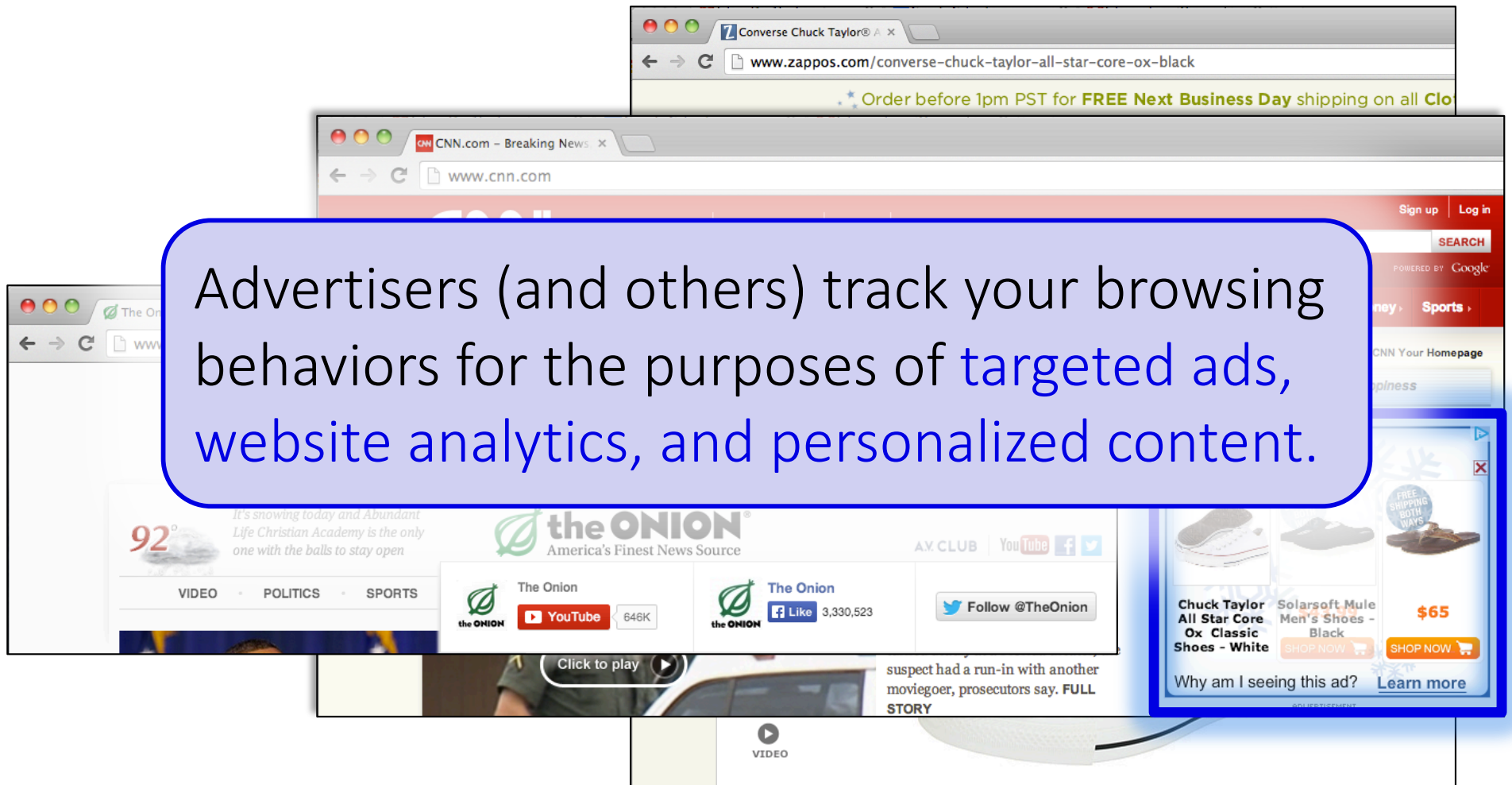
Why Not Always Strict Checking?

- Why might the referer header be suppressed?
 - Stripped by the organization's network filter
 - Stripped by the local machine
 - Stripped by the browser for HTTPS → HTTP transitions
 - User preference in browser
 - Buggy browser
- Web applications can't afford to block these users
- Many web application frameworks include CSRF defenses today

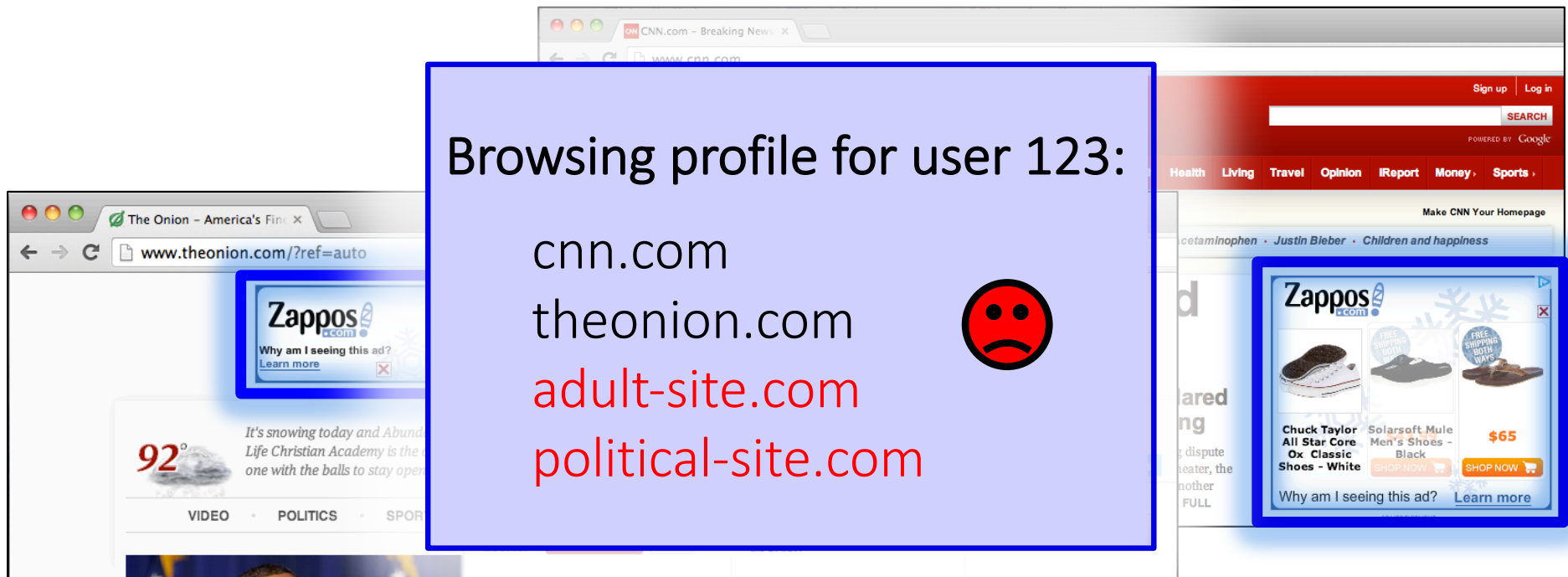
Web Privacy

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



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 Wall Street Journal
A Journal investigating business

CNN
Your Privacy
Big dep
By
Hid
all to be put up
The file consists
identifies her as

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.

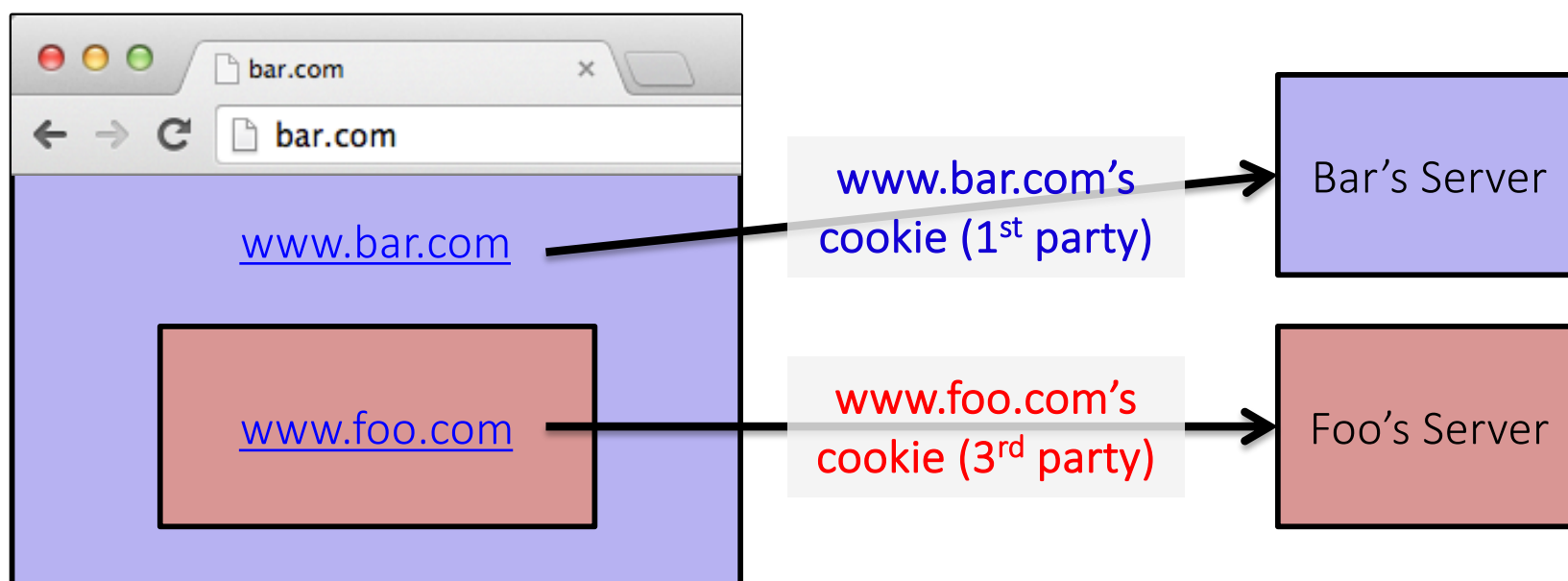
Log In

als
tion

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

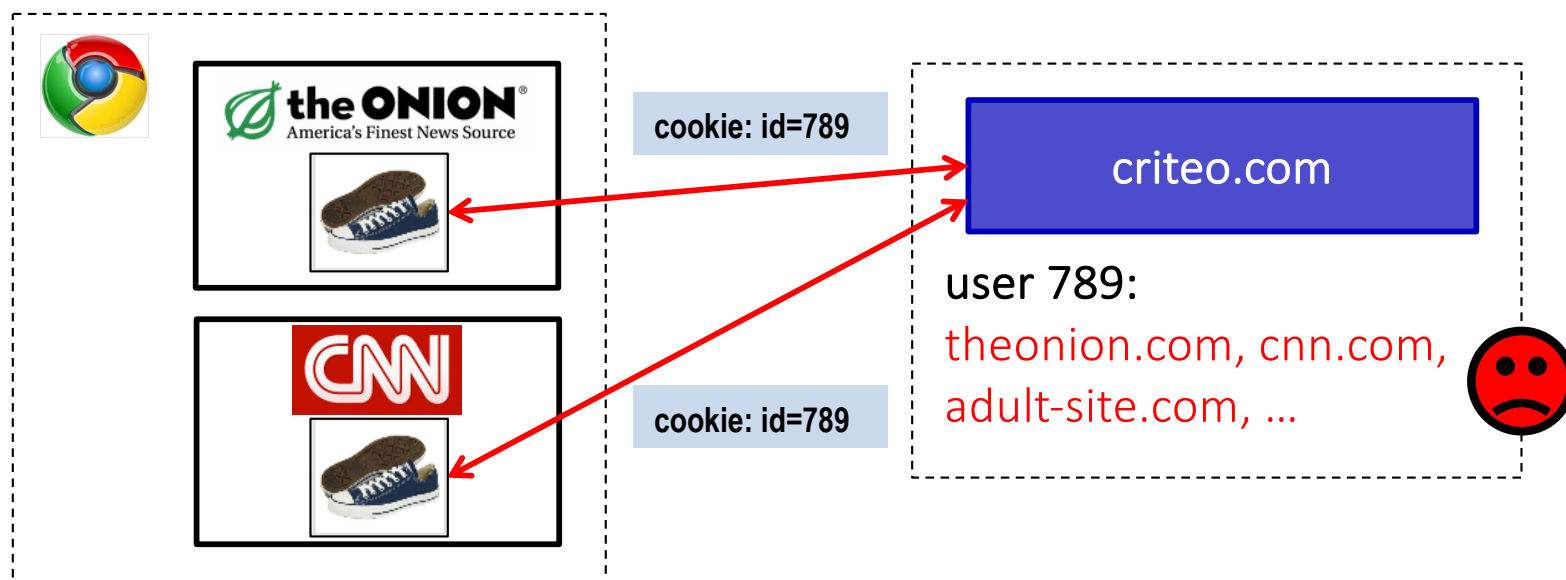
First and Third Parties

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



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!)



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

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

Only **anonymous data** will be collected by this site.



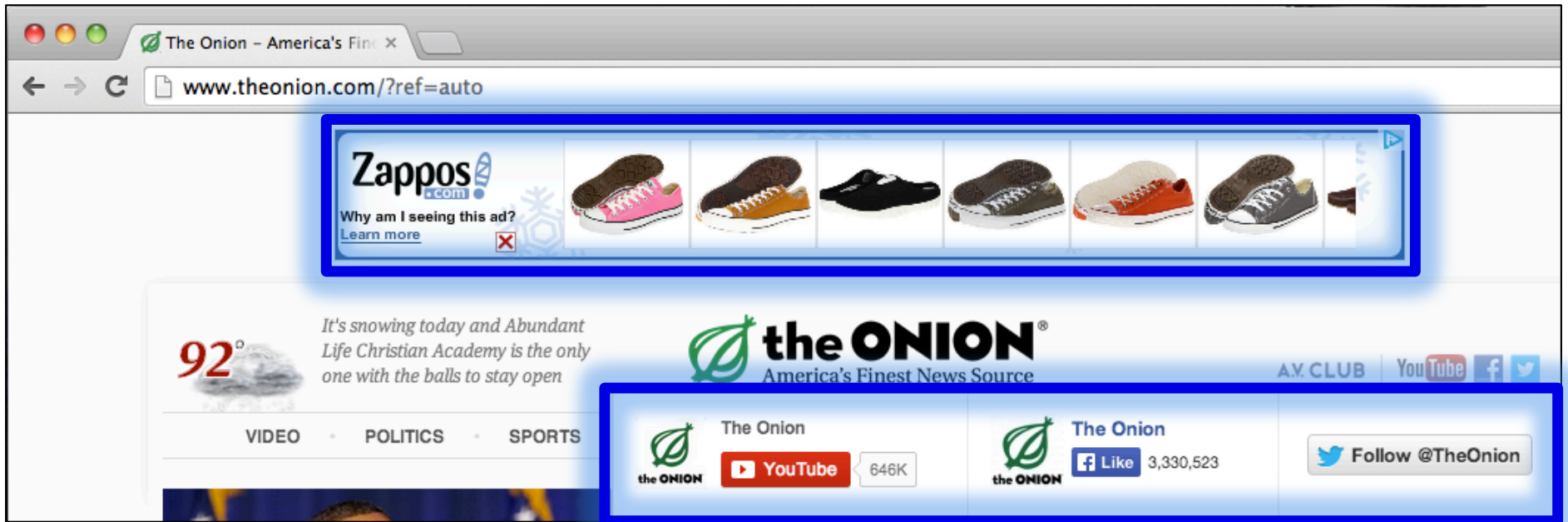
A paper reporting the statistical results of this experiment is now available: [How Unique Is Your Browser?](#), Proceedings of the Privacy Enhancing Technologies Symposium (PETS 2010), Springer Lecture Notes in Computer Science.

[Learn about Panopticlick and web tracking.](#)

[The Panopticlick Privacy Policy.](#)

[Learn about the Electronic Frontier Foundation.](#)

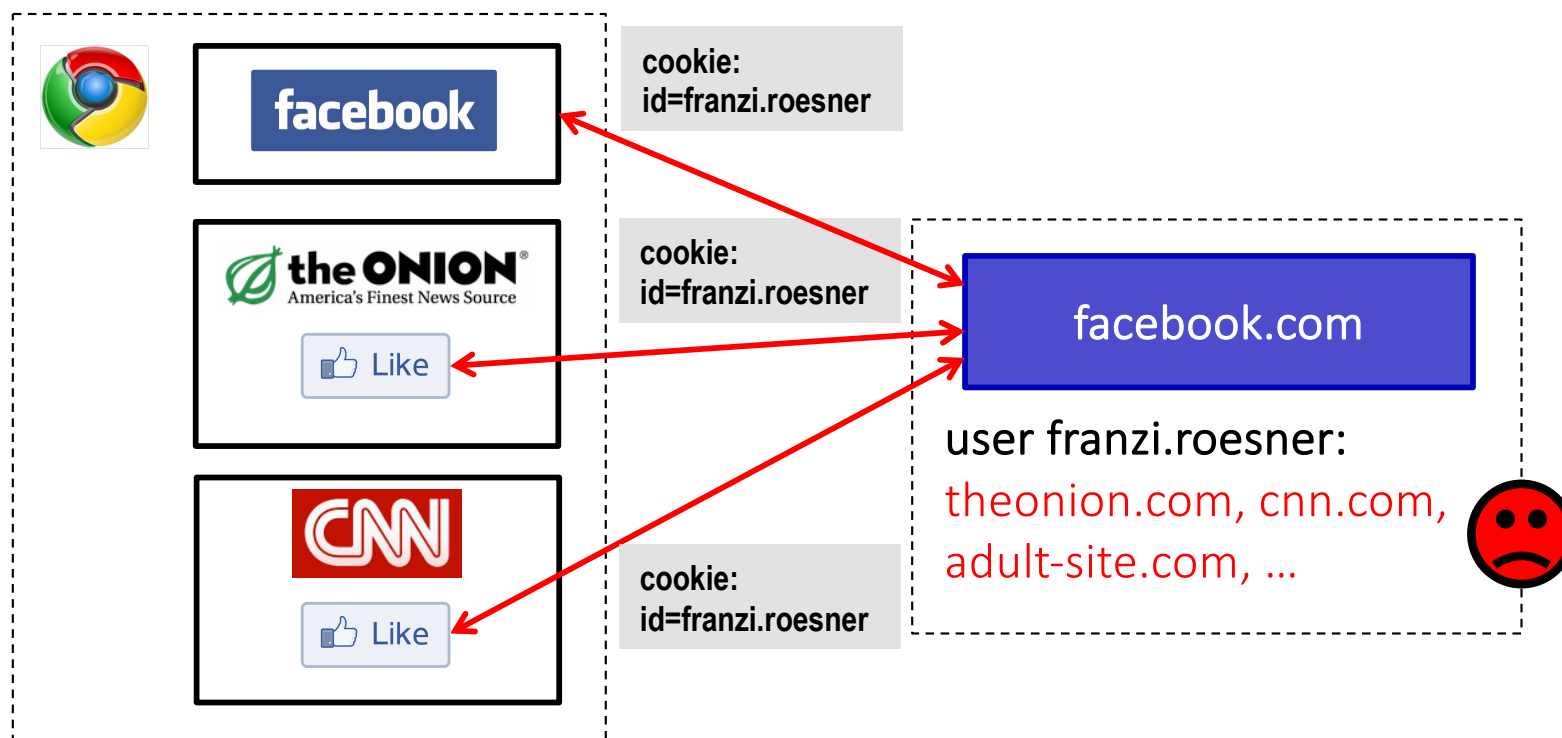
Other Trackers?



“Personal” Trackers



Personal Tracking



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