Web UI Attacks & Privacy

CMSC 23200, Spring 2025, Lecture 13

Grant Ho

University of Chicago, 05/06/2025

(Slides adapted from Blasé Ur, Peyrin Kao, Vern Paxson, and Zakir Durumeric)

Logistics

- Assignment 5 released either Fri / Sat (May 9 / 10)
  - Due Thursday, May 15 by 11:59pm
  - Schedule change due to VM outage
  - No TA office hours this week

- Discussion Section #5 tomorrow (May 7)

Outline

- UI Attacks
  - Clickjacking Attacks
  - Phishing Attacks

- Web Privacy: Online Tracking

Misleading Users

- UI Attacks: trick the victim into thinking they are taking an **intended** action, when they are actually taking a **malicious** action
  - Clickjacking: Trick the victim into clicking on some website element
  - Phishing: Impersonate another entity & trick victim into performing specific malicious actions (e.g., giving sensitive information)

- Key Issue: Browser assumes clicks & keystrokes = *clear indication of user's intended actions*
  - Constitutes part of the user's *trusted path*

Clickjacking

- Trick the victim into clicking on something from the attacker by hiding one frame (origin A) on-top or undernearth another (origin B)

- Why steal clicks?
  - Download a malicious program
  - Like a YouTube video
  - Delete an online account

- Why steal keystrokes?
  - Steal passwords
  - Steal credit card numbers
  - Steal personal info

Clickjacking Example

Suppose you use *cheapbank.com*… and they have a transfer page!

URL: `https://cheapbank.com/transfer.html?receiver=...`

Resulting webpage in browser (includes CSRF token)

Example from: https://developer.mozilla.org/en-US/docs/Web/Security/Attacks/Clickjacking

Clickjacking Example

Attacker on *shady-pet-supplies.com* creates a webpage with the following HTML & CSS:

HTML:

```
<button id="fake-button">Click here for a free kitten!</button>
<iframe width="800" height="200“ src="https://cheapbank.com/transfer.html?receiver=attacker"></iframe>
```

CSS:

```
#fake-button {
  position: absolute; top: 185px; left: 90px;     <------ Overlay attack button exactly over framed button
}
```

Clickjacking Example

shady-pet-supplies.com

Get a free kitten!

https://cheapbank.com/transfer.html?receiver=...

My bank

Transfer all your money?

SOP prevents *shady-pet-supplies.com* from interacting with embedded iframe – but user allowed to click & interact however they want!

Clickjacking Example

Attacker on *shady-pet-supplies.com* creates a webpage with the following HTML & CSS:

HTML:

```
<button id="fake-button">Click here for a free kitten!</button>
<iframe width="800" height="200“ src="https://cheapbank.com/transfer.html?receiver=attacker"></iframe>
```

CSS:

```
iframe { opacity: 0; }        <----- Invisible iframe contents

#fake-button {
  position: absolute; top: 185px; left: 90px;     <------ Overlay attack button exactly over framed button
}
```

Clickjacking Example

shady-pet-supplies.com

iframe = top most element,
but hidden / invisible with:
iframe { opacity: 0; }

Get a free kitten!

https://cheapbank.com/transfer.html?receiver=...

My bank

Transfer all your money?

Clickjacking Example

shady-pet-supplies.com

Clickjacking: Multiple Attack Variants

- By placing an invisible iframe of `target.com` *over* some enticing content, a malicious web server can fool a user into taking unintended action on `target.com` …

- By placing a visible iframe of `target.com` *under* the *attacker's own invisible iframe*, a malicious web server can "steal" user input (keystrokes)
  - Input text will be entered on the attacker site's iframe/origin

Defenses:
Prevent Other Sites from Framing You!

Attacker implements clickjacking by placing target's page (e.g., Twitter) in a "frame" inside their own page. Otherwise they wouldn't overlap.

Defenses: CSP or HTTP `X-Frame-Options`

web browser

example.com

HTTP response from server:

HTTP/1.1 200 OK

…

Content-Security-Policy: frame-ancestors <u>'none'</u>;

…

<iframe src='example.com'>
will cause an error

frame-ancestors 'self' ;
means only example.com
can frame page

Outline

- UI Attacks
  - Clickjacking Attacks
  - Phishing Attacks

- Web Privacy: Online Tracking

Phishing

- Masquerade as a reputable entity & trick the user into performing malicious actions, such as divulging login credentials

- Often easier than attacking the security of a system directly
  - Just get the user to tell you their password or download & run your malicious software

PayPal

Dear vern we are making a few changes

View Online

PayPal

Your Account Will Be Closed !

Hello, Dear vern

Your Account Will Be Closed , Until We Here From You . To Update Your Information . Simply click on the web address below

What do I need to do?

Confirm My Account Now

Date: Thu, 9 Feb 2017 07:19:40 -0600

From: PayPal <alert@gnc.cc>

Subject: [Important] : This is an automatic message to : (vern)

To: vern@aciri.org

ern". Emails from PayPal will always address you by your

This email was sent to vern.

PayPal

Dear vern we are making a few changes

View Online

PayPal

Your Account Will Be Closed !

Hello, Dear vern

Your Account Will Be Closed , Until We Here From You . To Update Your Information . Simply click on the web address below

What do I need to do?

Confirm My Account Now

Help **Contact** **Security**

How do I know this is not a Spoof email?

Spoof or 'phishing' emails tend to have generic greetings such as "Dearvern". Emails from PayPal will always address you by your first and last name.

Find out more here.

This email was sent to vern.

Open "universalkids.com.br/re.php" in a new window

evenxi.com

Log in to your PayPal account

PayPal

Email

Password

Log In

Forgot your email or password?

Sign Up

About | Account Types | Fees | Privacy | Security | Contact | Legal | Developers

evenxi.com

Log in to your PayPal account

PayPal

gaga@lady.com

••••••••••••

Log In

Forgot your email or password?

Sign Up

About | Account Types | Fees | Privacy | Security | Contact | Legal | Developers

PayPal, Inc.

Log in to your PayPal account

PayPal

Email

Password

Log In

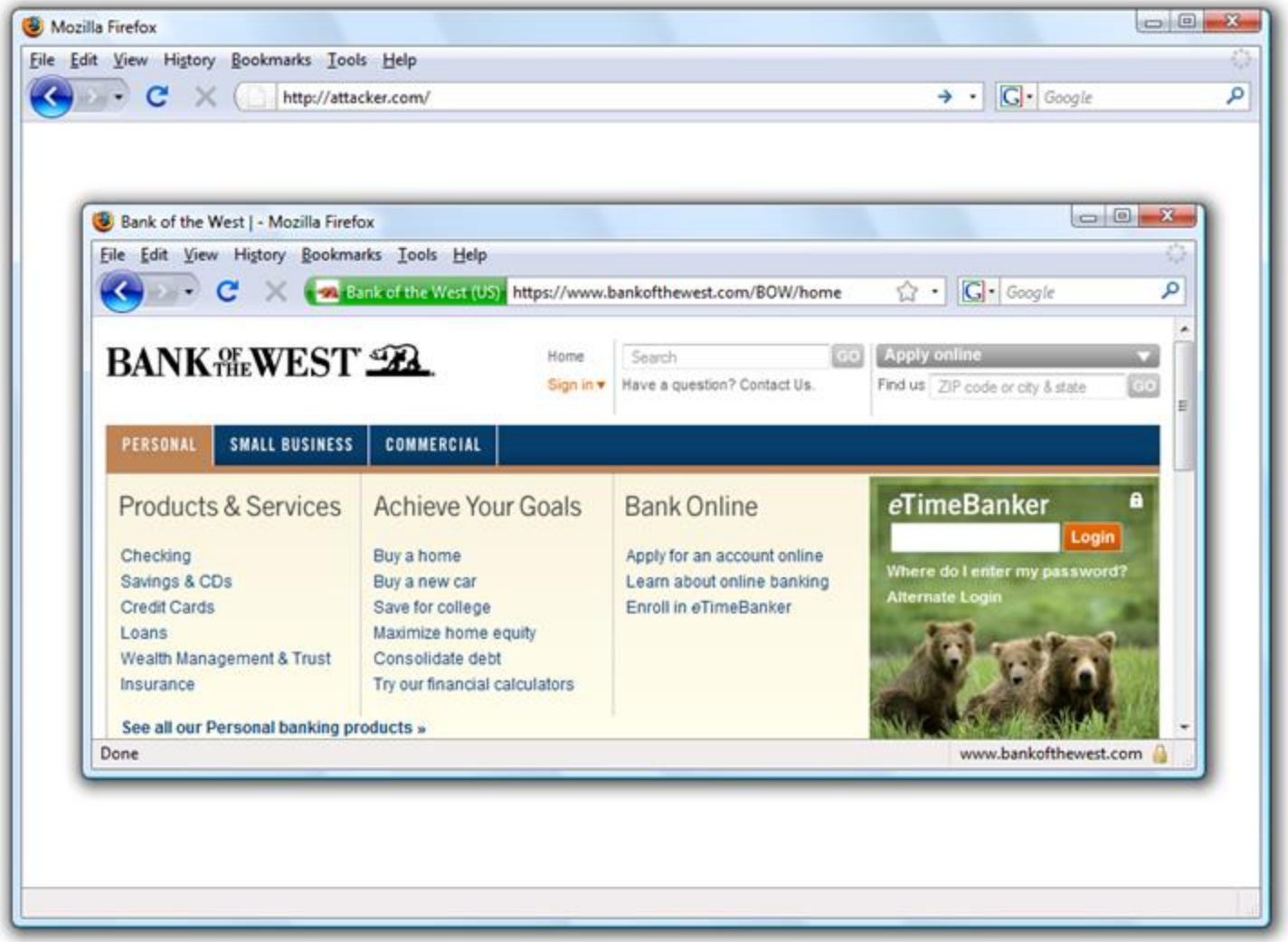
Having trouble logging in?

Sign Up

Contact Us Privacy Legal Worldwide

Lots of Phishing Strategies

Browser-in-browser attack: The attacker simulates the entire web browser with JavaScript



Internationalized Domain Names (IDN)

- Domain names consist of ASCII characters
- Hostnames containing Unicode characters are transcoded to subset of ASCII consisting of letters, digits, and hyphens called punycode
- Allows registering domains with foreign characters!
    - münchen.example.com → xn--mnchen-3ya.example.com

Phishing: IDN homograph attack

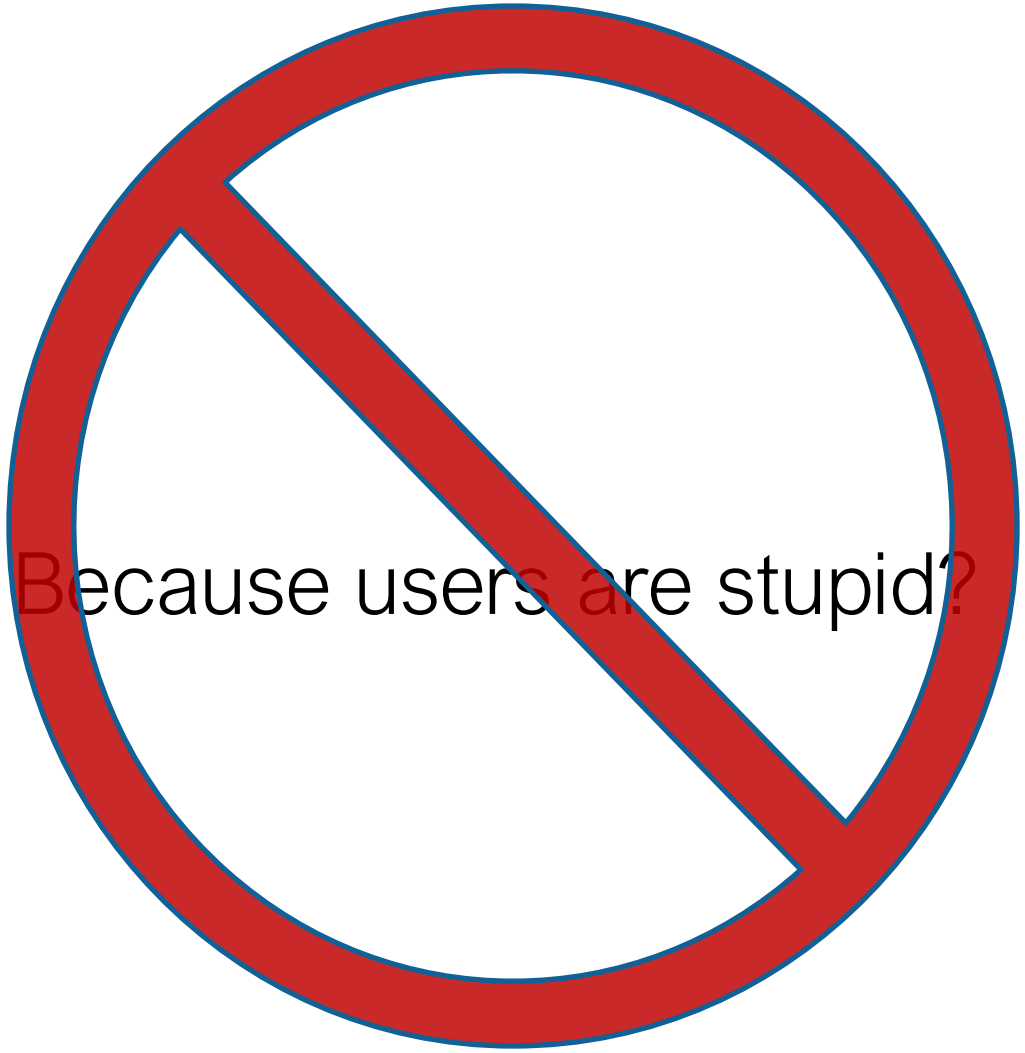
- Many Unicode characters are difficult to distinguish from common ASCII characters

apple.com vs. apple.com

xn--pple-43d.com

apple.com

Why does phishing work?

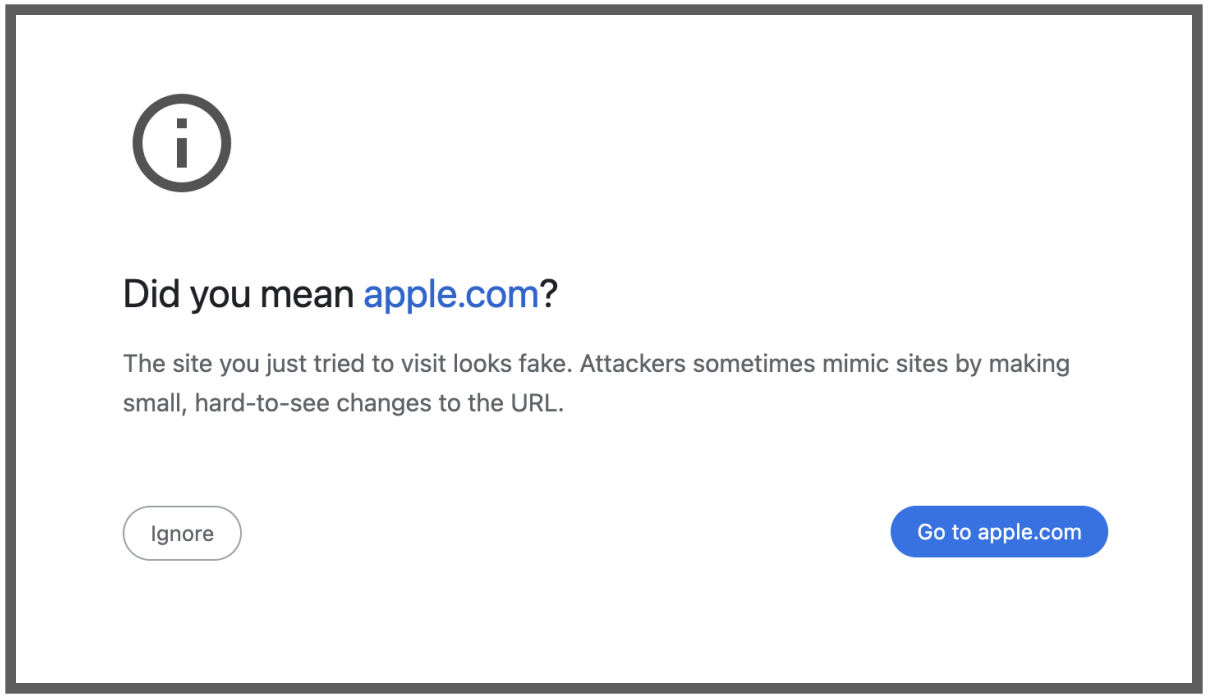


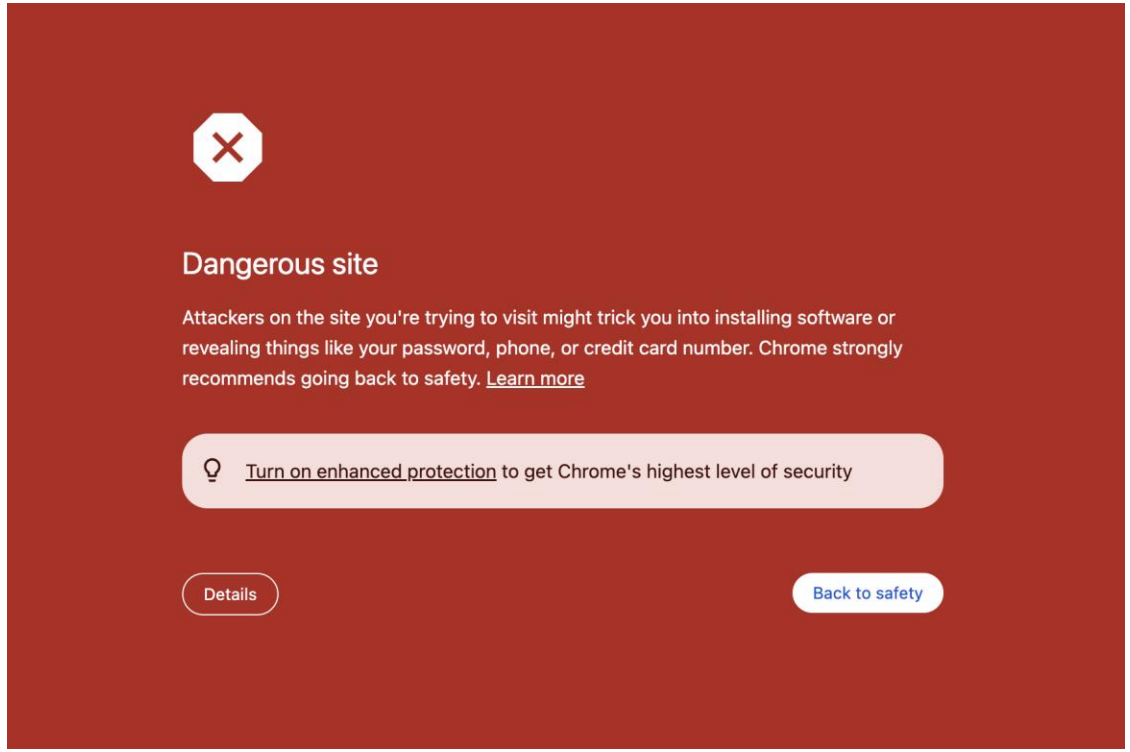
Why does phishing work?

- User mental model vs. reality
  - Browser security model too hard to understand!
  - Phishing is hard to spot even if you’re an expert!
- The easy path is insecure; the secure path takes extra effort
- Risks are rare
- Users tend not to suspect malice; they find benign interpretations and have been *acclimated to failure*

Phishing Defenses

- Detection & Blocklists (e.g., Google Safe Browsing)





Phishing Defenses

- Detection & Blocklists (e.g., Google Safe Browsing)
- Next week:
  - Password Managers (for credential phishing)
  - Multi-factor authentication (your friend Duo!)

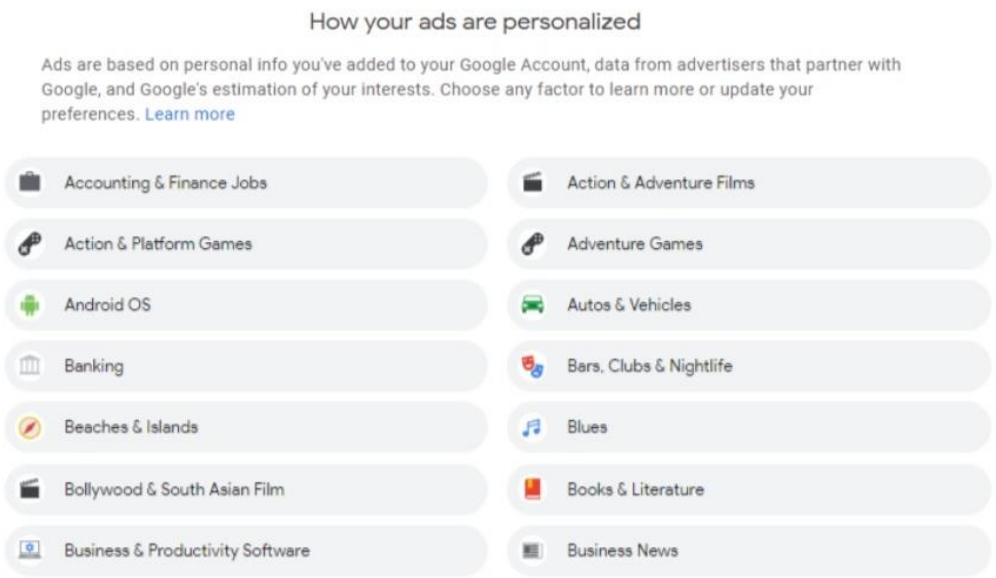
Outline

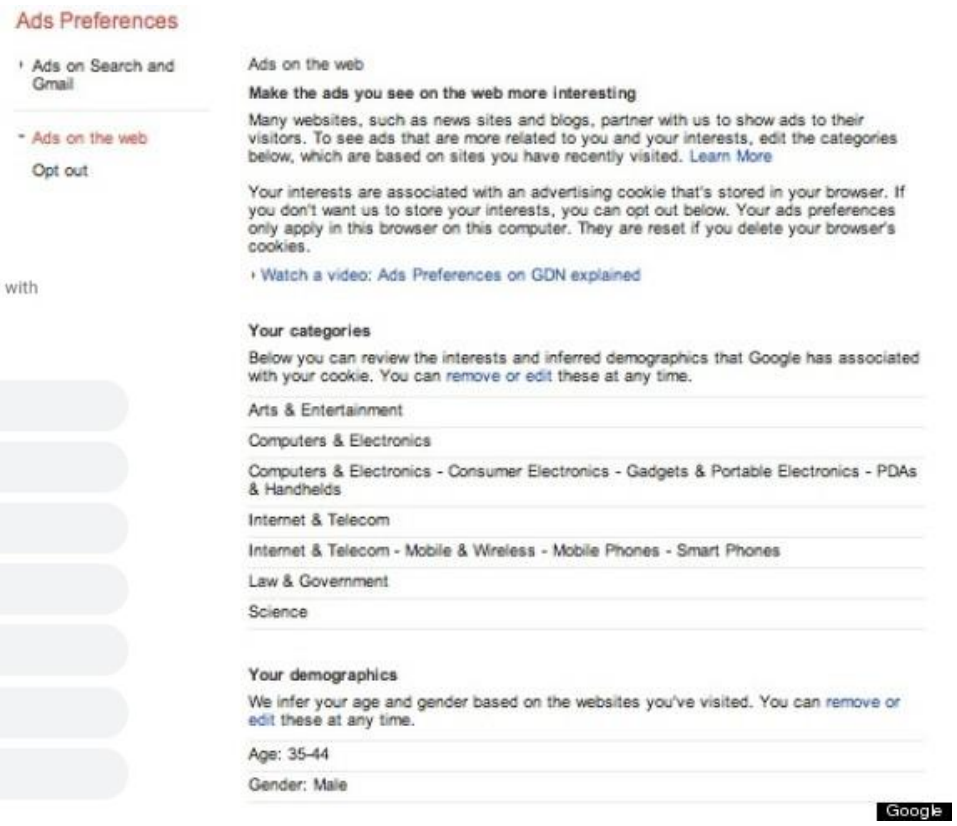
- UI Attacks
  - Clickjacking Attacks
  - Phishing Attacks

- Web Privacy: Online Tracking

Online Tracking

- Advertisers want to show you advertisements targeted to your interests and demographics



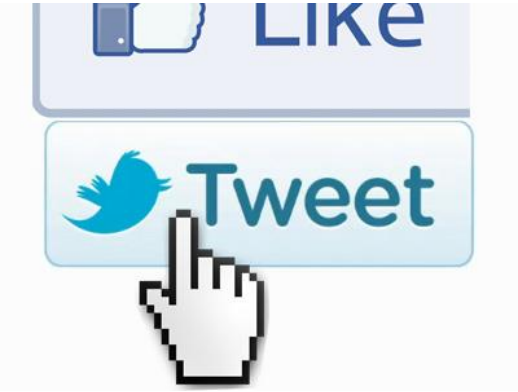


Data-Driven Inferences

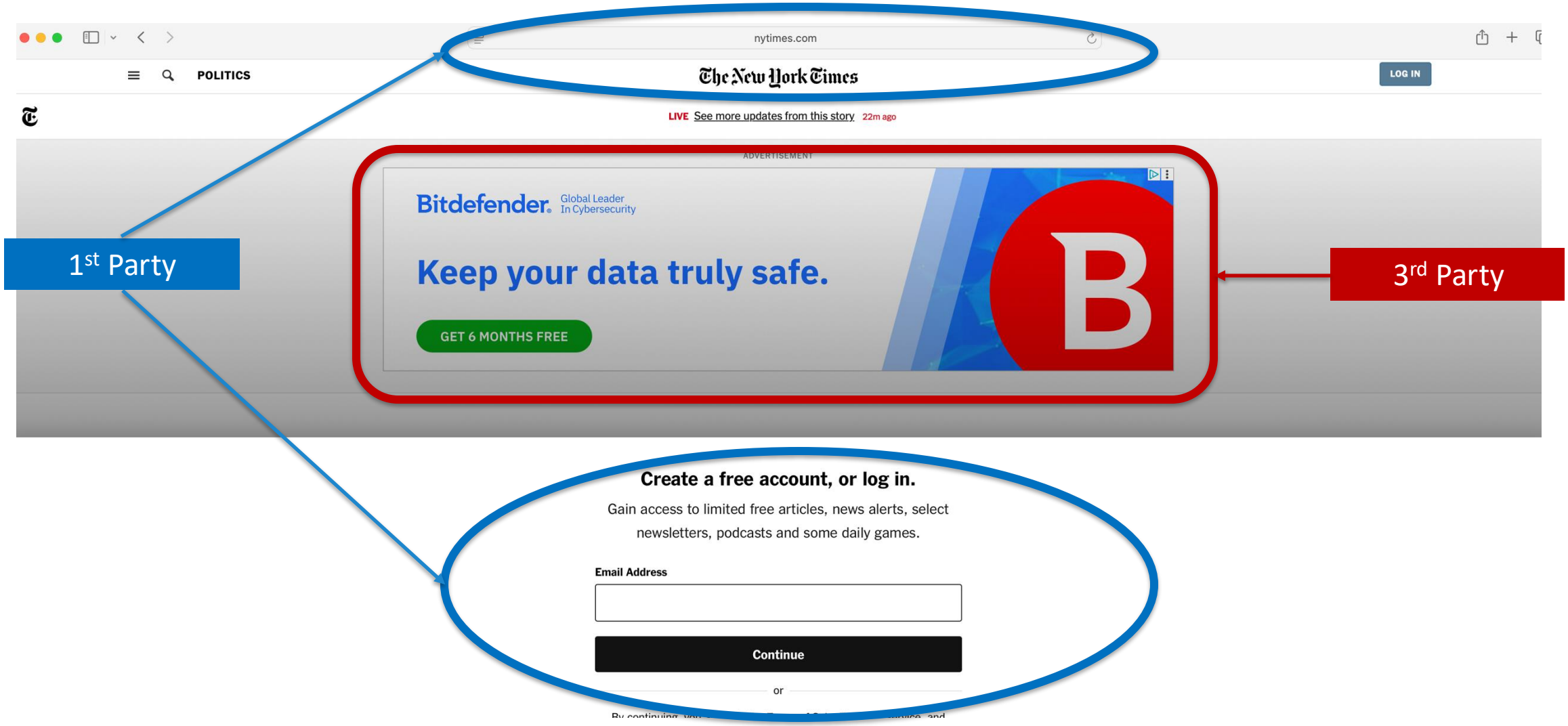
You might like dogs!

Online Tracking

- First party: the site you are visiting (address in the URL bar)
  - First-party tracking (on search engines, shopping sites)
  - Login/Session cookies
- Third party: other sites (origins) embedded/contacted by the first party site you're visiting
  - Third-party tracking (ads on lots of sites)

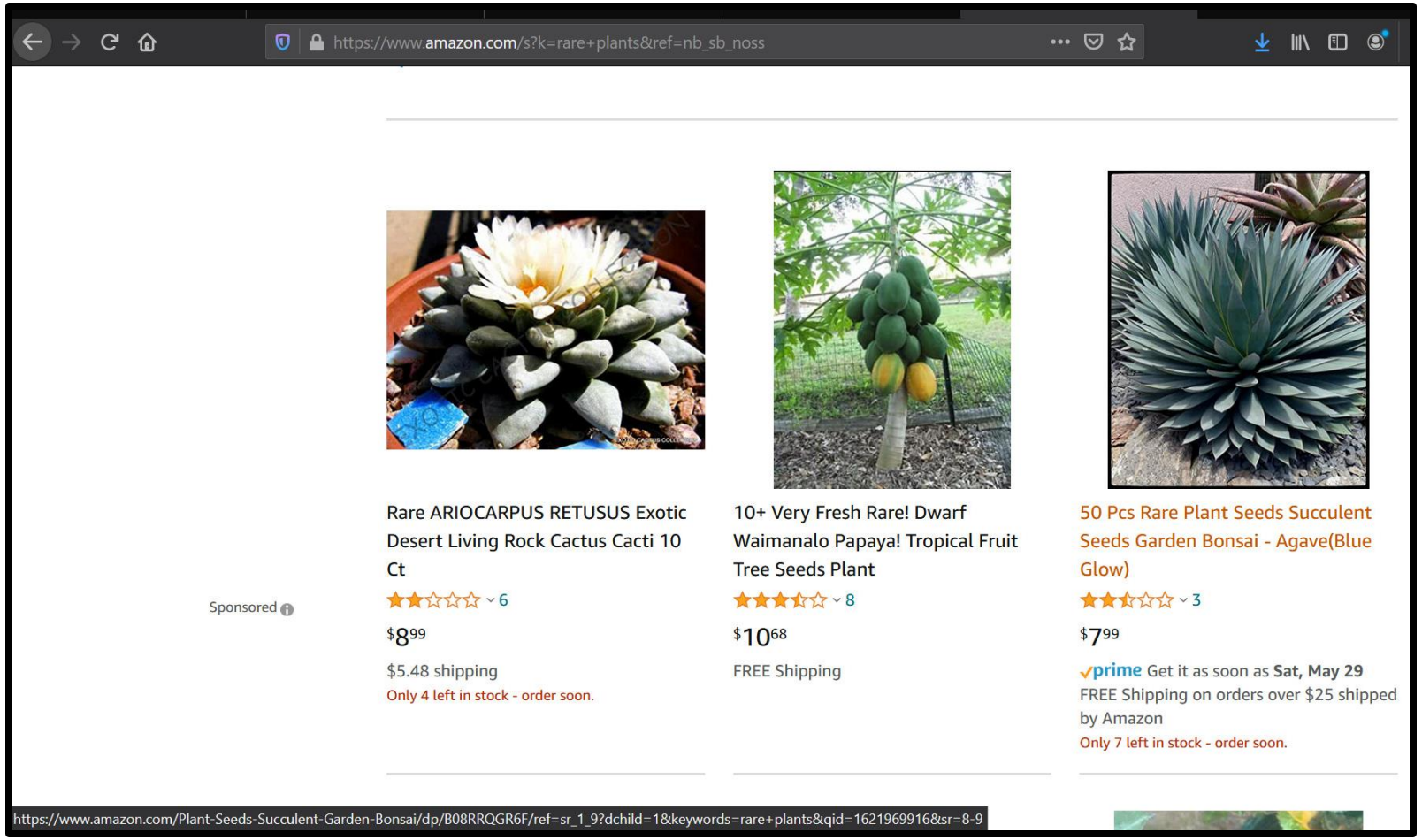


Online Tracking

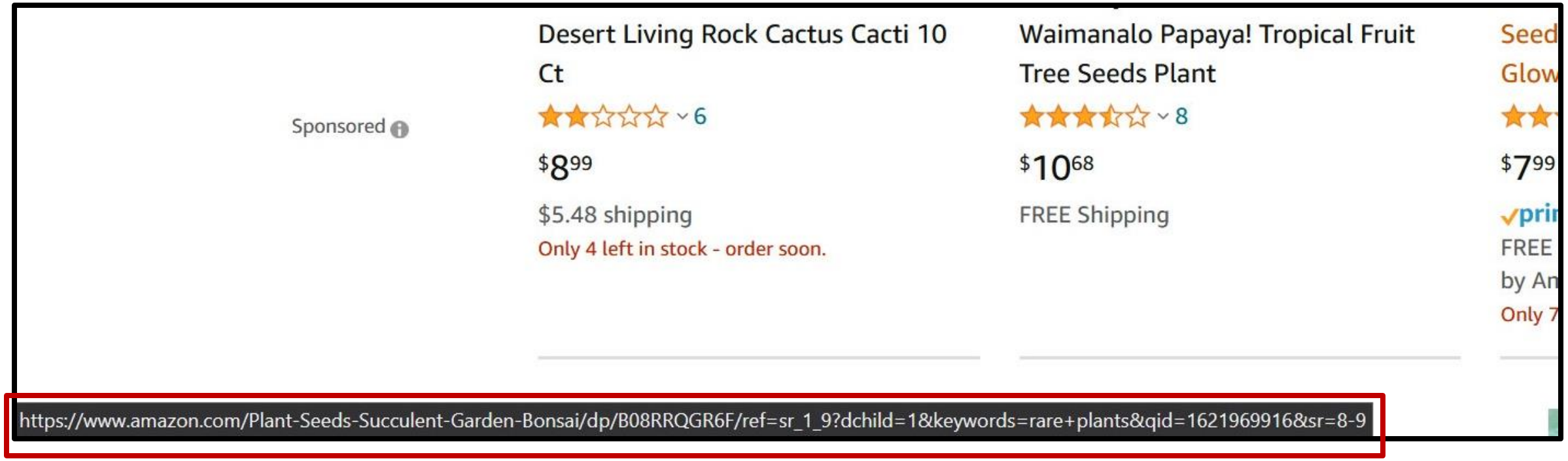


Mechanics of First-Party Online Tracking

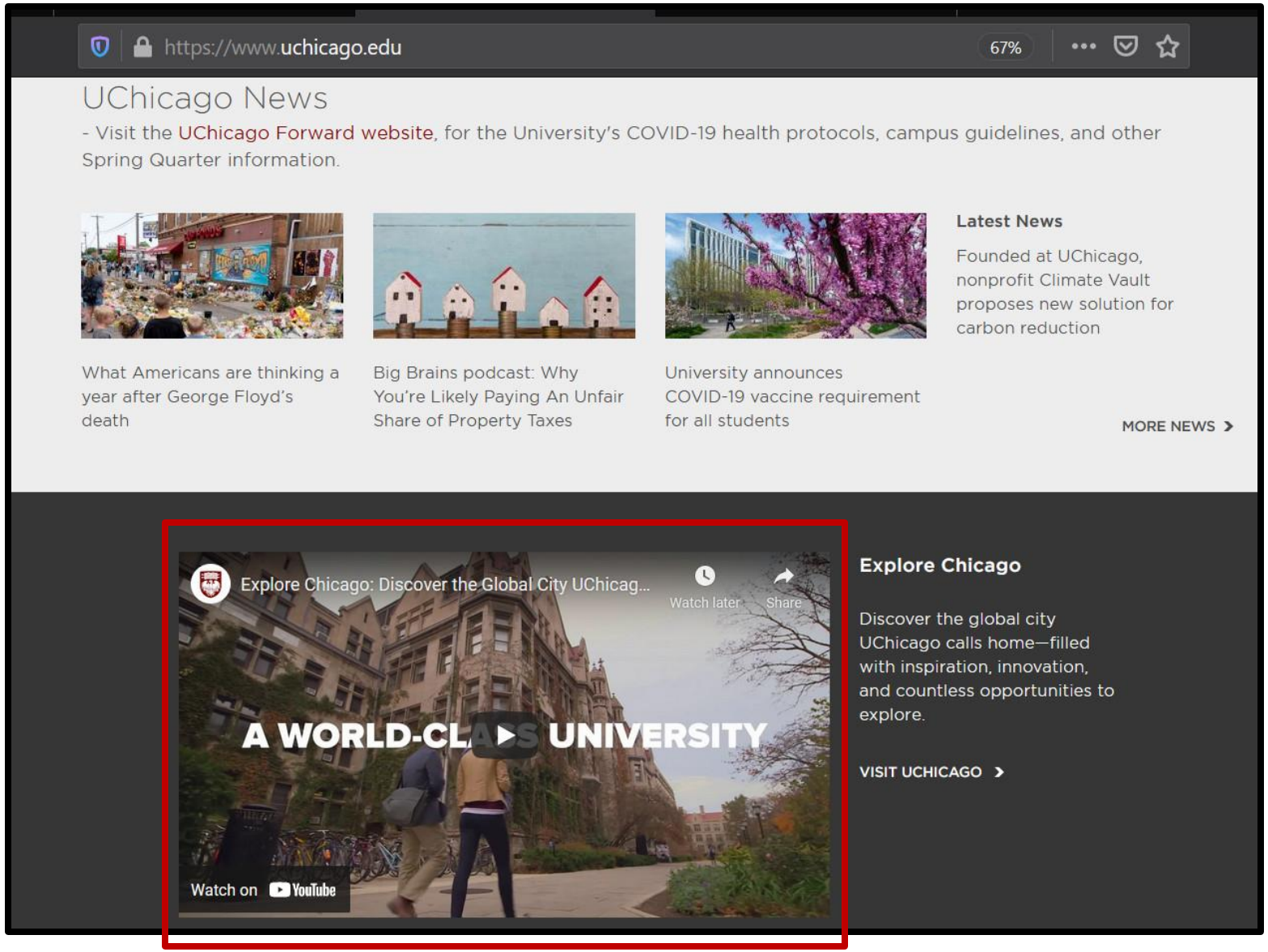
- Use cookies, JavaScript, URL parameters to track



Mechanics of First-Party Online Tracking



Mechanics of Third-Party Online Tracking



Details of What's Happening in HTTP (**Request**)

Request Headers (735 B) Raw

```
GET / HTTP/2
Host: www.uchicago.edu
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefo
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Connection: keep-alive
Cookie: uchicago-prod_last_visit=1306604446; uchicago-prod_last_activity=1621964446;
Upgrade-Insecure-Requests: 1
If-Modified-Since: Tue, 25 May 2021 17:40:36 GMT
TE: Trailers
```

Details of What's Happening in HTTP (**Request**)

Request Headers (735 B) Raw

```
GET / HTTP/2
Host: www.uchicago.edu
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefo
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Connection: keep-alive
Cookie: uchicago-prod_last_visit=1306604446; uchicago-prod_last_activity=1621964446;
Upgrade-Insecure-Requests: 1
If-Modified-Since: Tue, 25 May 2021 17:40:36 GMT
TE: Trailers
```

Details of What's Happening in HTTP (**Request**)

Request Headers (735 B) Raw

```
GET / HTTP/2
Host: www.uchicago.edu
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefo
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Connection: keep-alive
Cookie: uchicago-prod_last_visit=1306604446; uchicago-prod_last_activity=1621964446;
Upgrade-Insecure-Requests: 1
If-Modified-Since: Tue, 25 May 2021 17:40:36 GMT
TE: Trailers
```

Details of What's Happening in HTTP (Cookies)

Image taken from https://networkencyclopedia.com/http-cookie/

Details of What's Happening in HTTP (**Response**)

Response Headers (1.078 KB) Raw

```
HTTP/2 200 OK
date: Tue, 25 May 2021 18:00:35 GMT
content-type: text/html; charset=UTF-8
server: Apache
x-frame-options: SAMEORIGIN
expires: Mon, 26 Jul 1997 05:00:00 GMT
pragma: no-cache
vary: Accept-Encoding
set-cookie: uchicago-prod_last_visit=1306605629; expires=Wed, 25-May-2022 18:00:29 G
set-cookie: uchicago-prod_last_activity=1621965629; expires=Wed, 25-May-2022 18:00:2
set-cookie: uchicago-prod_tracker=%7B%220%22%3A%22index%22%2C%22token%22%3A%2226944a
set-cookie: uchicago-prod_csrf_token=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT;
set-cookie: uchicago-prod_csrf_token=86d47d8690aa7646e1628dd095cd5b464db16bd3; expir
last-modified: Tue, 25 May 2021 18:00:29 GMT
content-encoding: gzip
x-varnish: 10696657 9201444
age: 5
via: 1.1 varnish (Varnish/5.2)
accept-ranges: bytes
X-Firefox-Spdy: h2
```

Details of What's Happening in HTTP (**Response**)

Response Headers (1.078 KB) Raw

```
HTTP/2 200 OK
date: Tue, 25 May 2021 18:00:35 GMT
content-type: text/html; charset=UTF-8
server: Apache
x-frame-options: SAMEORIGIN
expires: Mon, 26 Jul 1997 05:00:00 GMT
pragma: no-cache
vary: Accept-Encoding
set-cookie: uchicago-prod_last_visit=1306605629; expires=Wed, 25-May-2022 18:00:29 G
set-cookie: uchicago-prod_last_activity=1621965629; expires=Wed, 25-May-2022 18:00:2
set-cookie: uchicago-prod_tracker=%7B%220%22%3A%22index%22%2C%22token%22%3A%2226944a
set-cookie: uchicago-prod_csrf_token=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT;
set-cookie: uchicago-prod_csrf_token=86d47d8690aa7646e1628dd095cd5b464db16bd3; expir
last-modified: Tue, 25 May 2021 18:00:29 GMT
content-encoding: gzip
x-varnish: 10696657 9201444
age: 5
via: 1.1 varnish (Varnish/5.2)
accept-ranges: bytes
X-Firefox-Spdy: h2
```

Persistent cookies!

https://www.uchicago.edu 67%

UChicago News

- Visit the UChicago Forward website, for the University's COVID-19 health protocols, campus guidelines, and other Spring Quarter information.

What Americans are thinking a year after George Floyd's death

Big Brains podcast: Why You're Likely Paying An Unfair Share of Property Taxes

University announces COVID-19 vaccine requirement for all students

Latest News

Founded at UChicago, nonprofit Climate Vault proposes new solution for carbon reduction

MORE NEWS >

Explore Chicago

Discover the global city UChicago calls home—filled with inspiration, innovation, and countless opportunities to explore.

VISIT UCHICAGO >

HTTP Headers (uchicago.edu → youtube.com)

Inspector | Console | Debugger | Style Editor | Performance | Memory | Network | Storage | Accessibility | Application | 13

Filter URLs | All | HTML | CSS | JS | XHR | Fonts | Images | Media | WS | Other | Disable Cache | No Throttling

Status	Met...	Domain	File	Initiator	Type	Transferred	Size
200	GET	www.uchica...	/	document	html	11.41 KB	39...
204	POST	www.youtub...	atr?ns=yt&el=embedded&cpn=ho5PKBh-	base.js:1023 (...	html	604 B	0 B
200	GET	www.youtub...	P-xlixF7B2U?autohide=1&fs=1&autoplay=	subdocument	html	21.81 KB	51...
200	GET	cdn.hypemar...	uchicagowww?width=1169&paginate=tru	a5b5e5.js:3 (s...	html	128.06 KB	12...
200	GET	cdn.hypemar...	popUpModalEndpoint	a5b5e5.js:3 (s...	html	10.99 KB	10...

5 requests | 229.65 KB / 172.86 KB transferred | Finish: 4.03 min | DOMContentLoaded: 451 ms | load: 1.70 s

Headers | Cookies | Request | Response | Timings | Security

Filter Headers | Block | Resend

Status	200 OK
Version	HTTP/3
Transferred	21.81 KB (51.50 KB size)
Referrer Policy	strict-origin-when-cross-origin

Response Headers (642 B) | Raw

```
HTTP/3 200 OK
content-type: text/html; charset=utf-8
x-content-type-options: nosniff
cache-control: no-cache, no-store, max-age=0, must-revalidate
pragma: no-cache
expires: Mon, 01 Jan 1990 00:00:00 GMT
date: Tue, 25 May 2021 18:00:36 GMT
strict-transport-security: max-age=31536000
permissions-policy: ch-ua-full-version=*, ch-ua-platform=*, ch-ua-platform-version=*, ch-u
content-encoding: br
server: ESF
x-xss-protection: 0
alt-svc: h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3
```

Request Headers (621 B) | Raw

```
GET /embed/P-xlixF7B2U?autohide=1&fs=1&autoplay=0&rel=0&modestbranding=1&showinfo=0&hd=1&e
Host: www.youtube.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Alt-Used: www.youtube.com
Connection: keep-alive
Referer: https://www.uchicago.edu/
Cookie: VISITOR_INFO1_LIVE=dACtKPaJViQ; PREF=tz=America.Chicago&f4=4000000; YSC=p2jSvxCMeI
Upgrade-Insecure-Requests: 1
TE: Trailers
```

HTTP Headers (uchicago.edu → youtube.com)

Inspector | Console | Debugger | Style Editor | Performance | Memory | Netw

Filter URLs | All

Status	Met...	Domain	File	Initiator	Type	Transferred	Size
200	GET	www.uchica...	/	document	html	11.41 KB	39...
204	POST	www.youtub...	atr?ns=yt&el=embedded&cpn=ho5PKBh-	base.js:1023 (...	html	604 B	0 B
200	GET	www.youtub...	P-xlixF7B2U?autohide=1&fs=1&autoplay=	subdocument	html	21.81 KB	51...
200	GET	cdn.hypemar...	uchicagowww?width=1169&paginate=tru	a5b5e5.js:3 (s...	html	128.06 KB	12...
200	GET	cdn.hypemar...	popUpModalEndpoint	a5b5e5.js:3 (s...	html	10.99 KB	10...

HTTP Headers (uchicago.edu → youtube.com)

Request Headers (621 B) Raw

```
GET /embed/P-xlixF7B2U?autohide=1&fs=1&autoplay=0&rel=0&modestbranding=1&showinfo=0&hd=1&e
Host: www.youtube.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Alt-Used: www.youtube.com
Connection: keep-alive
Referer: https://www.uchicago.edu/
Cookie: VISITOR_INFO1_LIVE=dACtKPaJViQ; PREF=tz=America.Chicago&f4=4000000; YSC=p2jSvxCMeI
Upgrade-Insecure-Requests: 1
TE: Trailers
```

HTTP Headers (uchicago.edu → youtube.com)

Request Headers (621 B) Raw

```
GET /embed/P-xlixF7B2U?autohide=1&fs=1&autoplay=0&rel=0&modestbranding=1&showinfo=0&hd=1&e
Host: www.youtube.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Alt-Used: www.youtube.com
Connection: keep-alive
Referer: https://www.uchicago.edu/
Cookie: VISITOR_INFO1_LIVE=dACtKPaJViQ; PREF=tz=America.Chicago&f4=4000000; YSC=p2jSvxCMeI
Upgrade-Insecure-Requests: 1
TE: Trailers
```

Putting It Together: Simple 3rd Party Tracking

- (Unless browser blocks it) third party gets its cookies
- (Unless browser blocks it) third party sees “referer” [sic]
- 1st party can choose to send info to third party via URL parameters (not a violation of Same Origin Policy!)
- 3rd party sees this information for **many** first parties (whoever embeds them!)
- In practice, advertising & 3rd party tracking much more complicated (lots of different 3rd parties involved)

Alternatives to Cookies for Tracking / Profiling

Various Side Channels

- Side channel: learning information through indirect means
- (Loophole has since mostly been closed)

```
a:visited {
  color: purple;
}
```

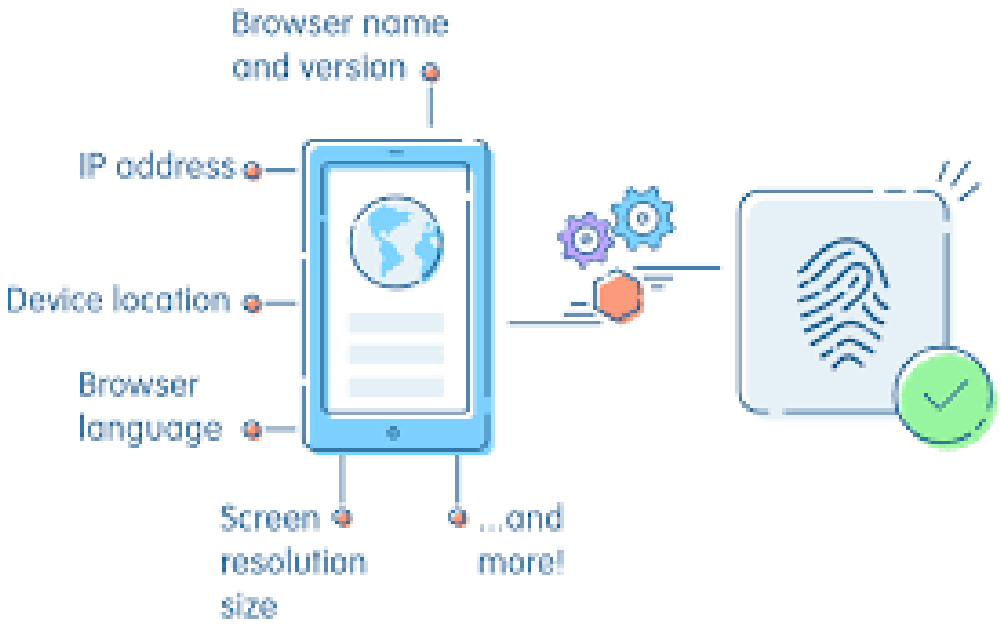
- link one
- second link
- link three (visited)
- fourth link

Browser Fingerprinting

- Use features of the browser that are relatively unique to your machine
  - Fonts
  - GPU model anti-aliasing (Canvas fingerprinting)
  - User-agent string
  - *(Often not)* IP address *(Why not?)*

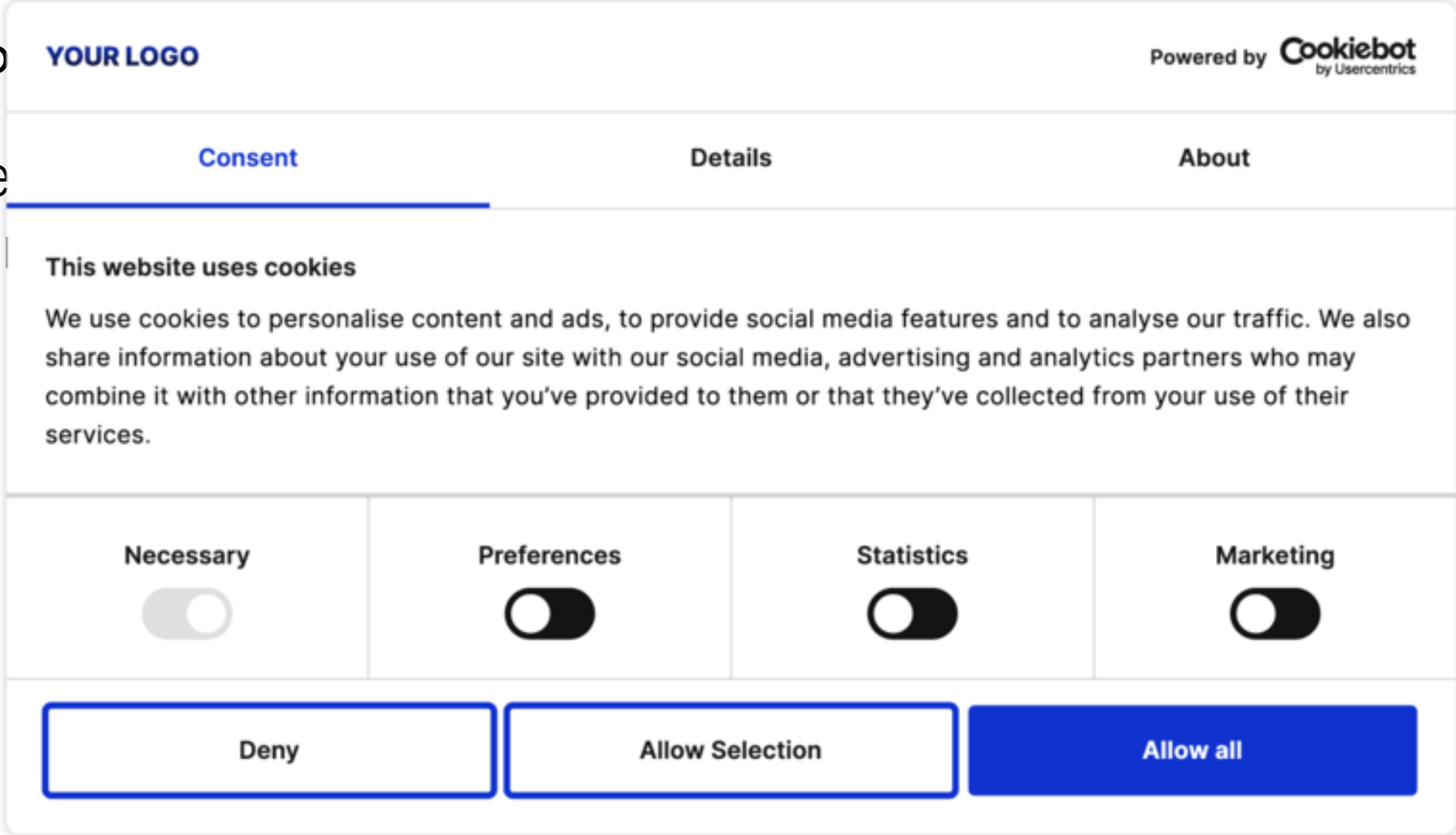
Browser Fingerprinting

- Use combination of device features as an identifier
- https://coveryourtracks.eff.org/



Various Legal & Regulatory Efforts

- GDP
  - Ne for 3rd pa



Various Legal & Regulatory Efforts

- GDPR (EU) & CCPA (California)
  - New laws to require explicit opt-in consent & transparency for 3rd party cookie use & tracking mechanisms

- Google originally aimed to completely phase out 3rd party cookies from the web by 2025 (unclear status now)

Google’s Topics API

https://www.theverge.com/2022/1/25/22900567/google-floc-abandon-topics-api-cookies-tracking

THE VERGE TECH REVIEWS SCIENCE CREATORS ENTERTAINMENT VIDEO MORE

GOOGLE POLICY TECH

Google abandons FLoC, introduces Topics API to replace tracking cookies

Google’s new concept assigns users five interests per week based on web activity

By Emma Roth | Updated Jan 25, 2022, 2:45pm EST

SHARE

Google’s Topics API

https://www.theverge.com/2022/1/25/22900567/google-floc-abandon-topics-api-cookies-tracking

EVERGE TWITTER FACEBOOK

Your browser will store these topics for three weeks before deleting them. Google says that these categories “are selected entirely on your device” and don’t involve “any external servers, including Google servers.” When you visit a website, Topics will show the site and its advertising partners just three of your interests, consisting of “one topic from each of the past three weeks.”

As noted on the Topics API GitHub page, there are currently about 350 available topics in its advertising taxonomy (although Google plans on adding anywhere from “a few hundred” to “a few thousand” eventually). Google says Topics won’t include any “sensitive categories” like race or gender. And if you’re using Chrome, the company is building tools to let you view and delete topics, as well as turn off the feature.