ECE458/ECE750T27: Computer Security

Web Security – Basics of Websites

Dr. Kami Vaniea,
Electrical and Computer Engineering
kami.vaniea@uwaterloo.ca

UNIVERSITY OF WATERLOO | FACULTY OF ENGINEERING

First, the news...

- First 5 minutes we talk about something interesting and recent
- You will not be tested on the news part of lecture
- You may use news as an example on tests
- Why do this?
    1. Some students show up late for various good reasons
    2. Reward students who show up on time
    3. Important to see real world examples

https://therecord.media/german-court-meta-tracking-tech

The Record.
Recorded Future® News

CREDIT: GREG BULLA / UNSPLASH

Suzanne Smalley

July 9th, 2025

News | News Briefs | Privacy

German court rules Meta tracking technology violates European privacy laws

A German court has ruled that Meta must pay €5,000 ($5,900) to a German Facebook user who sued the platform for embedding tracking technology in third-party websites — a ruling that could open the door to large fines down the road over data privacy violations relating to pixels and similar tools.

The Regional Court of Leipzig in Germany ruled Friday that Meta tracking pixels and software development kits embedded in countless websites and apps collect users' data without their consent and violate the continent's General Data Protection Regulation (GDPR).

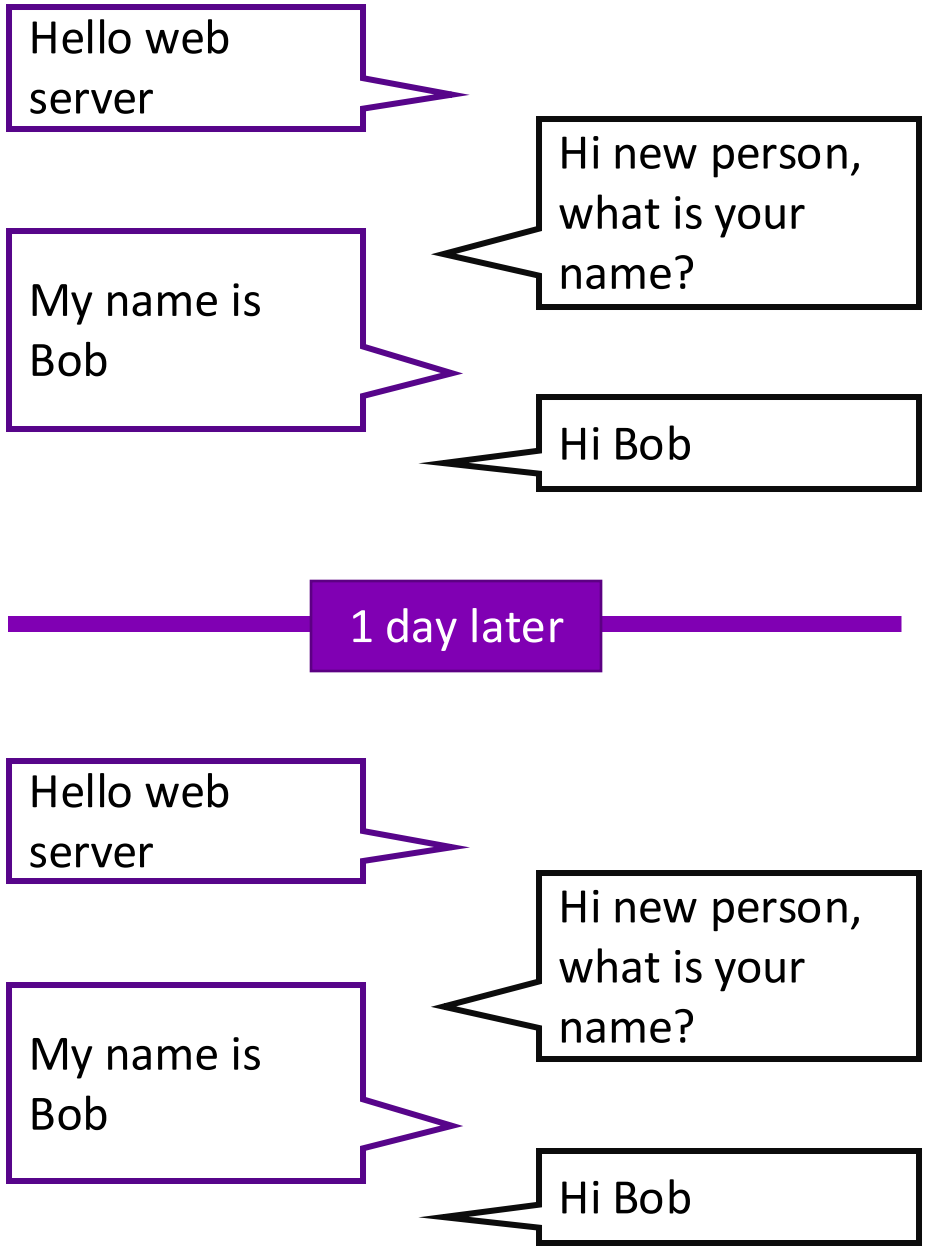
The ruling in favor of the plaintiff sets a precedent which the court acknowledged will allow countless other users to sue without "explicitly demonstrating individual damages," according to a Leipzig Regional Court press release.

"Every user is individually identifiable to Meta at all times as soon as they visit the third-party websites or use an app, even if they have not logged in via the Instagram and Facebook account," the press release said.

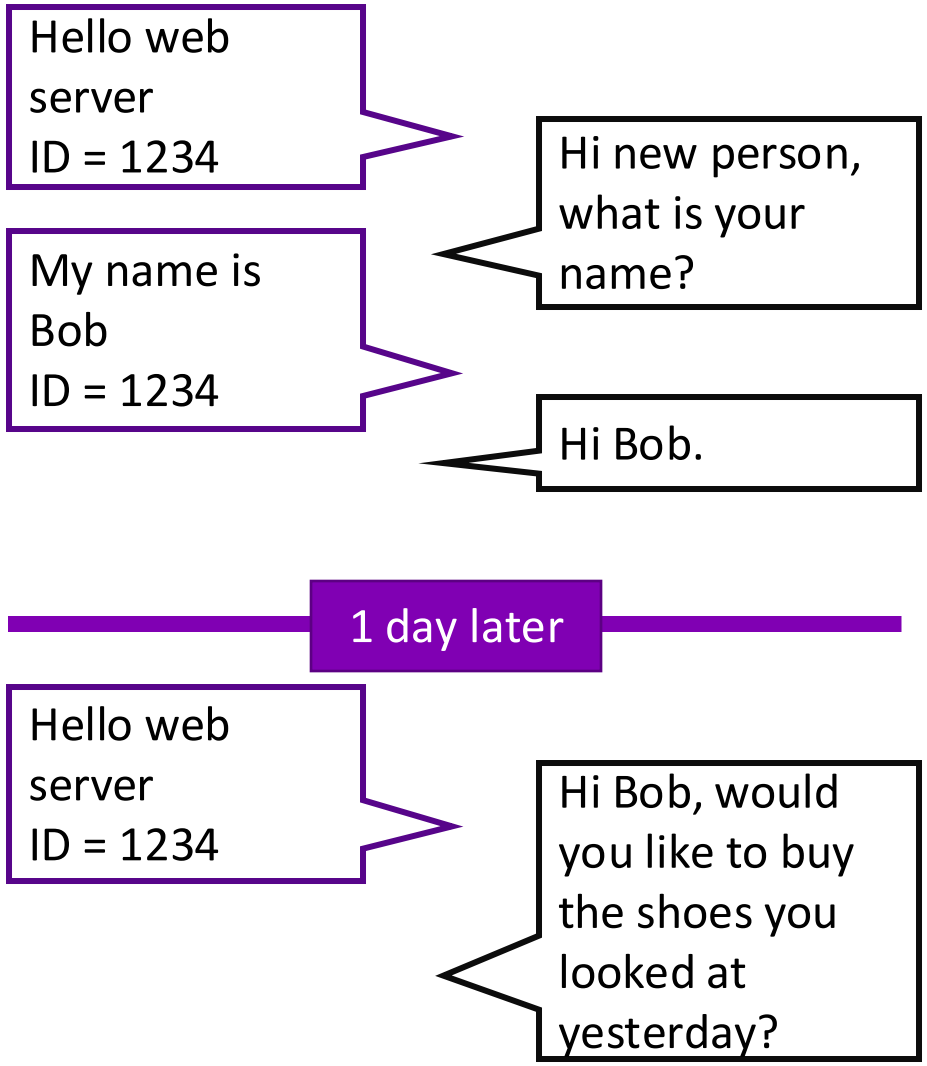
DESIGNING THE WEB COOKIE

Heavily based on Lou Montulli's "The reasoning behind Web Cookies"

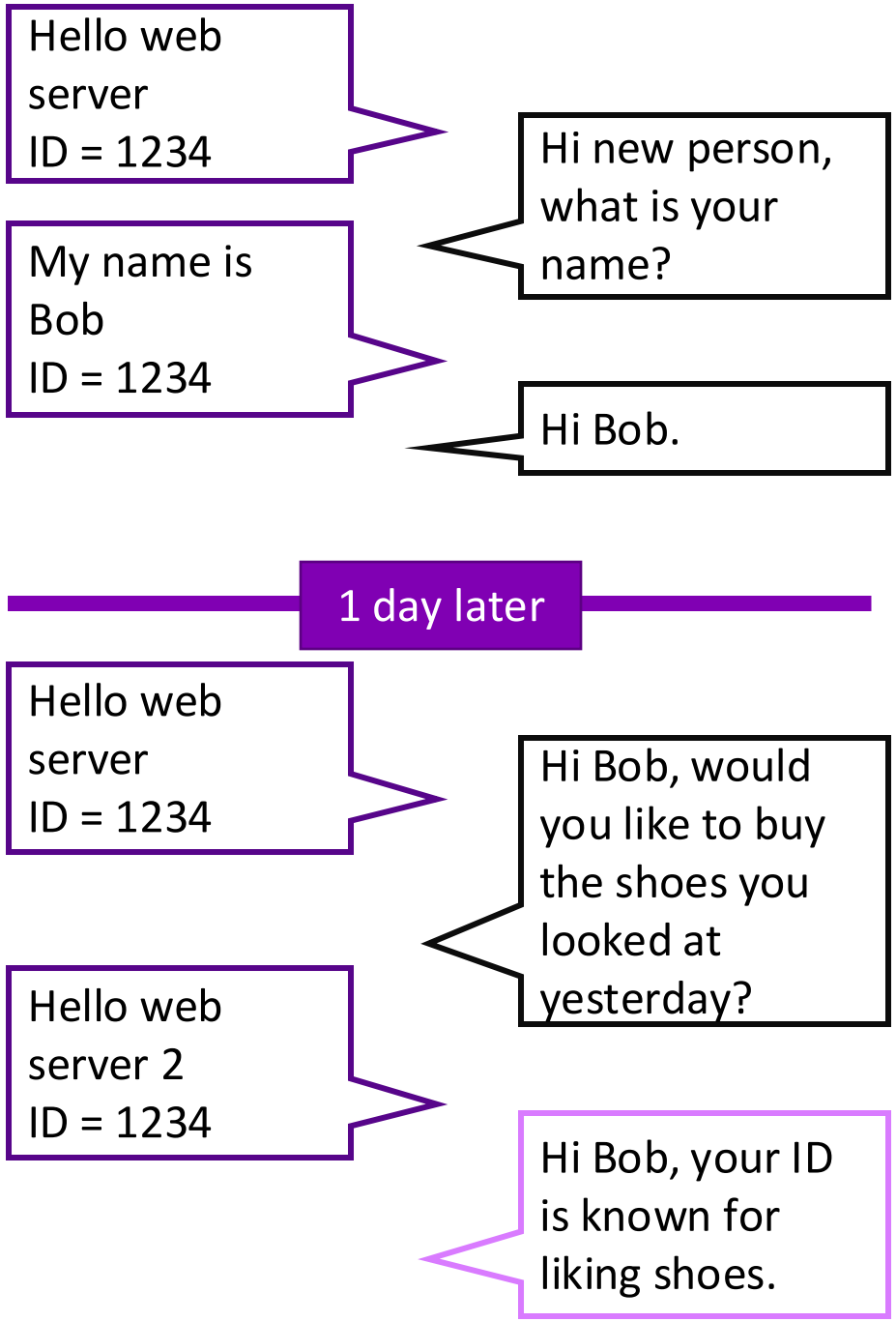
The year is 1994 and there is a problem... the internet has no ability to remember a person between page reloads.



There is an obvious easy solution... Give each browser a unique identifier.

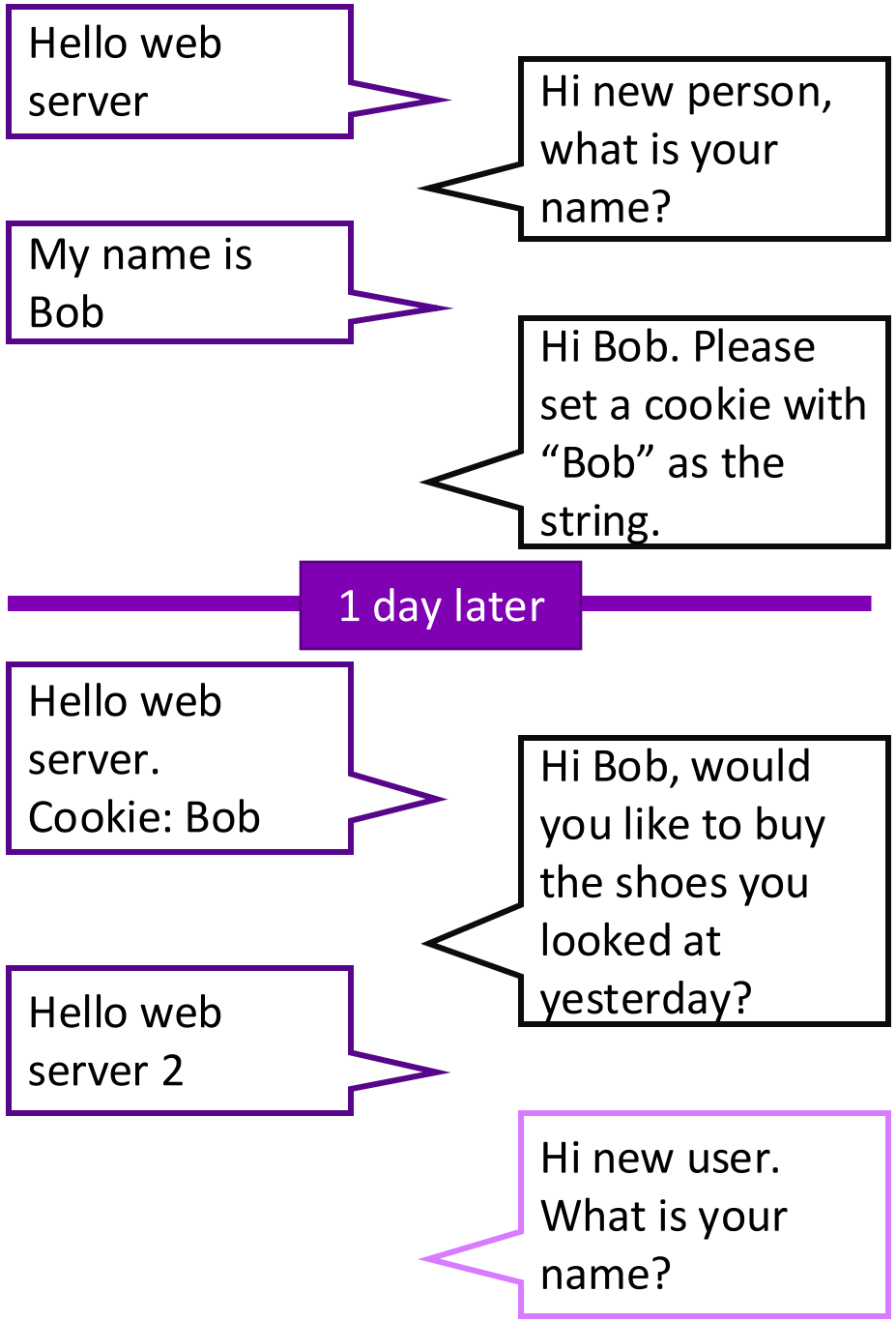


The problem with the obvious solution is privacy. Tracking would be possible with no visibility or control.



Instead Netscape implemented cookies.

Small text strings the server can ask the browser to remember and give back later.



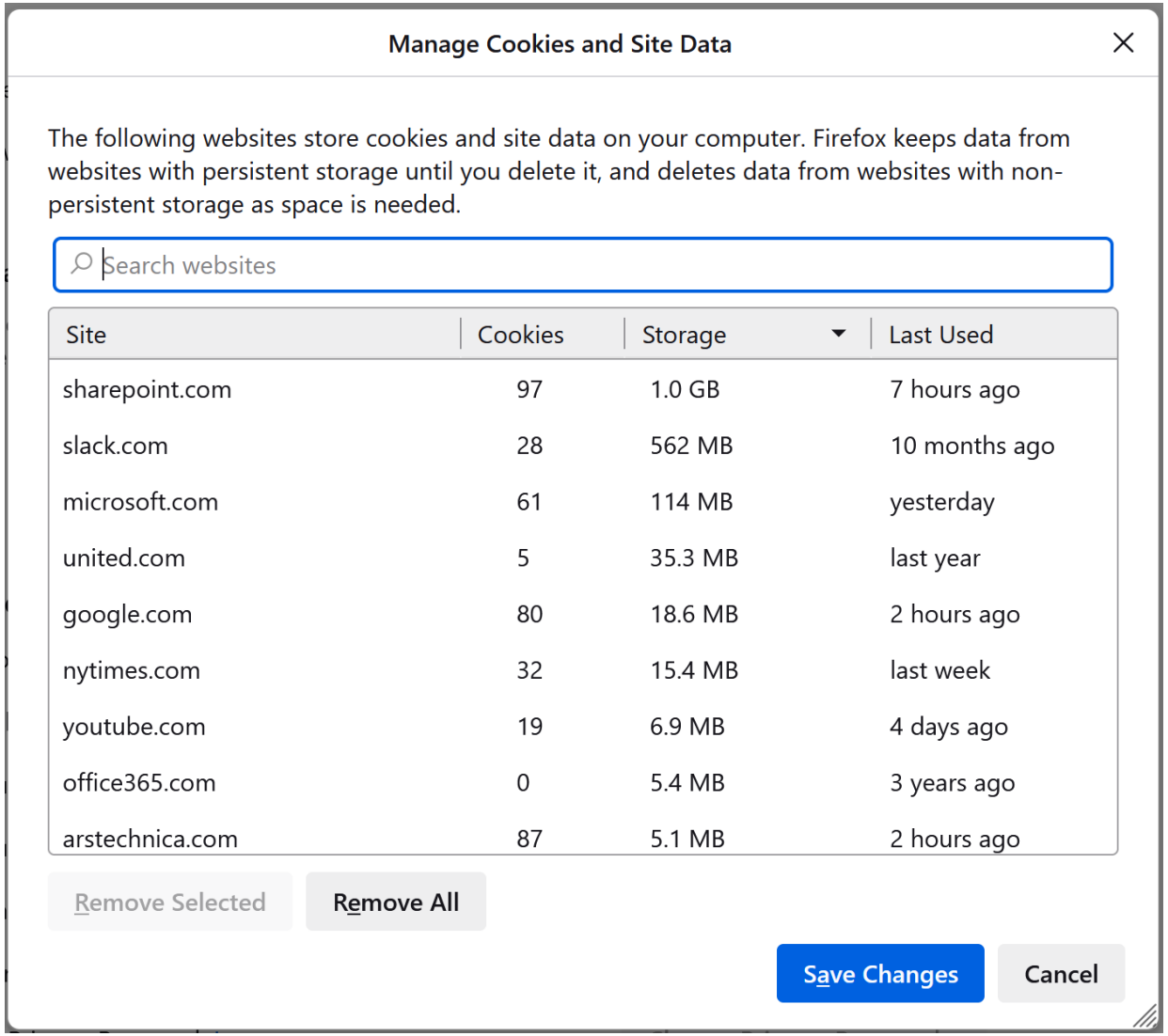
Cookies have some awesome properties for privacy

- Client (not server) manages cookies, so tracking is visible to the client
- Third party tracking is client visible too
- Opt-out (delete) option on a per-site basis
- Only readable by site that set it
- Allows for public discussion of tracking because the public can see the tracking happening

- … Android/IOS both went with the unique ID option

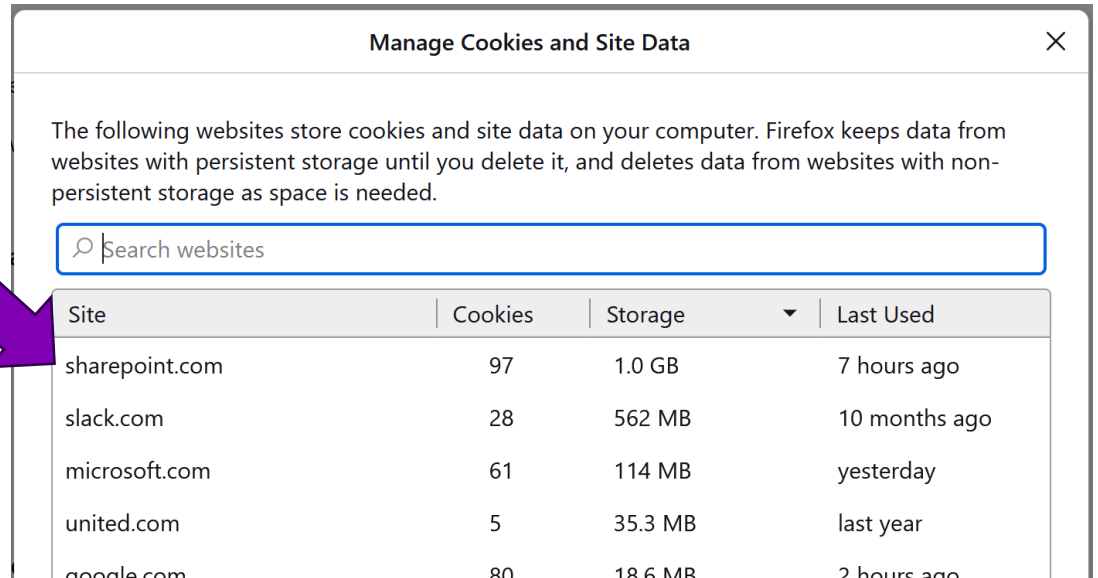
Look at your own cookies

- Cookies are managed client-side
- You can view all your cookies in most browsers
- It is impossible to silently track people using cookies, because the cookie must be stored by the browser

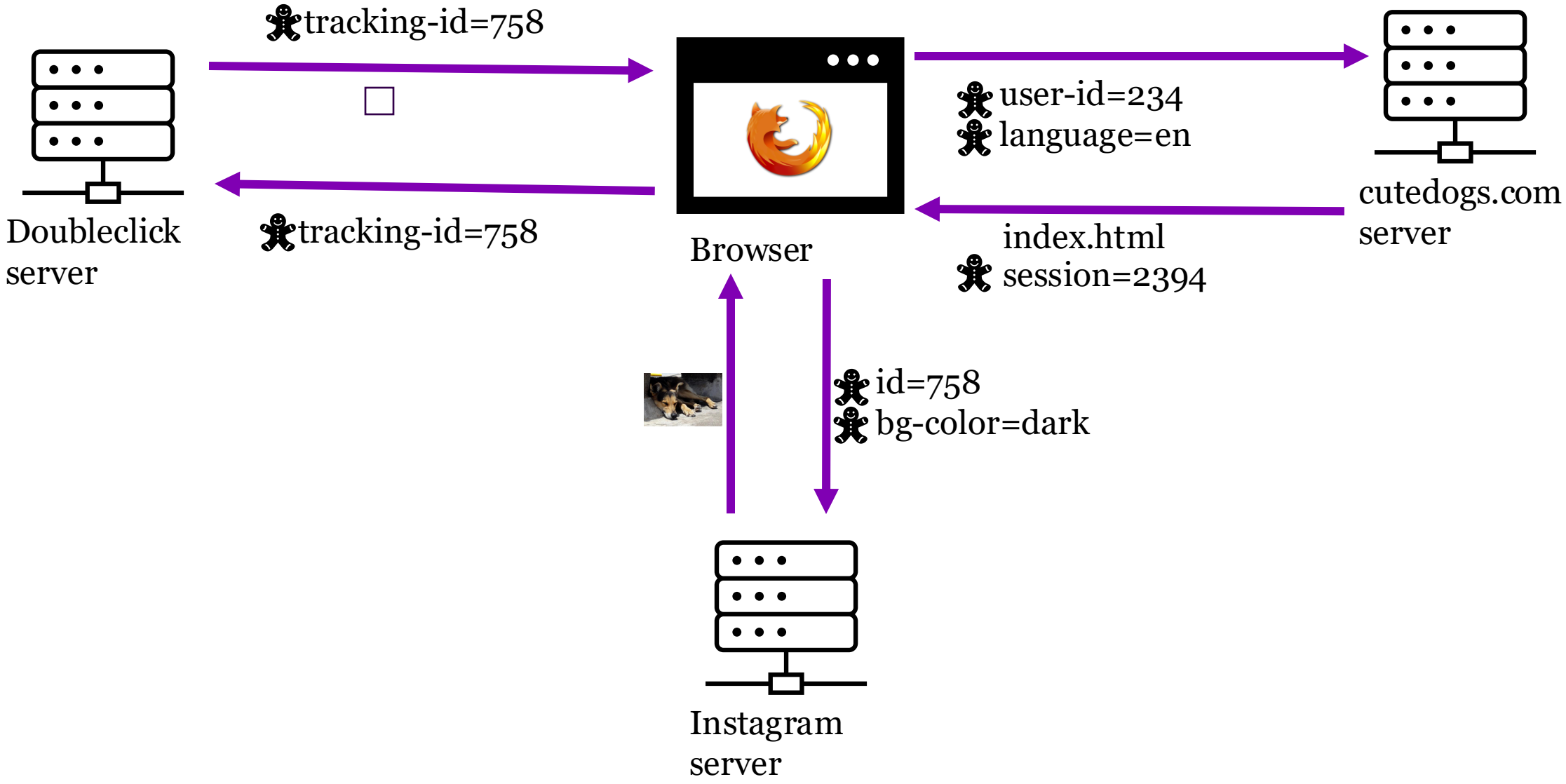


Security and Privacy Properties of Cookies

- Lets load Cute Dogs again, but this time look closely at the connections being made
- Cookies are **only** sent to a page if the domain matches the cookie's set domain



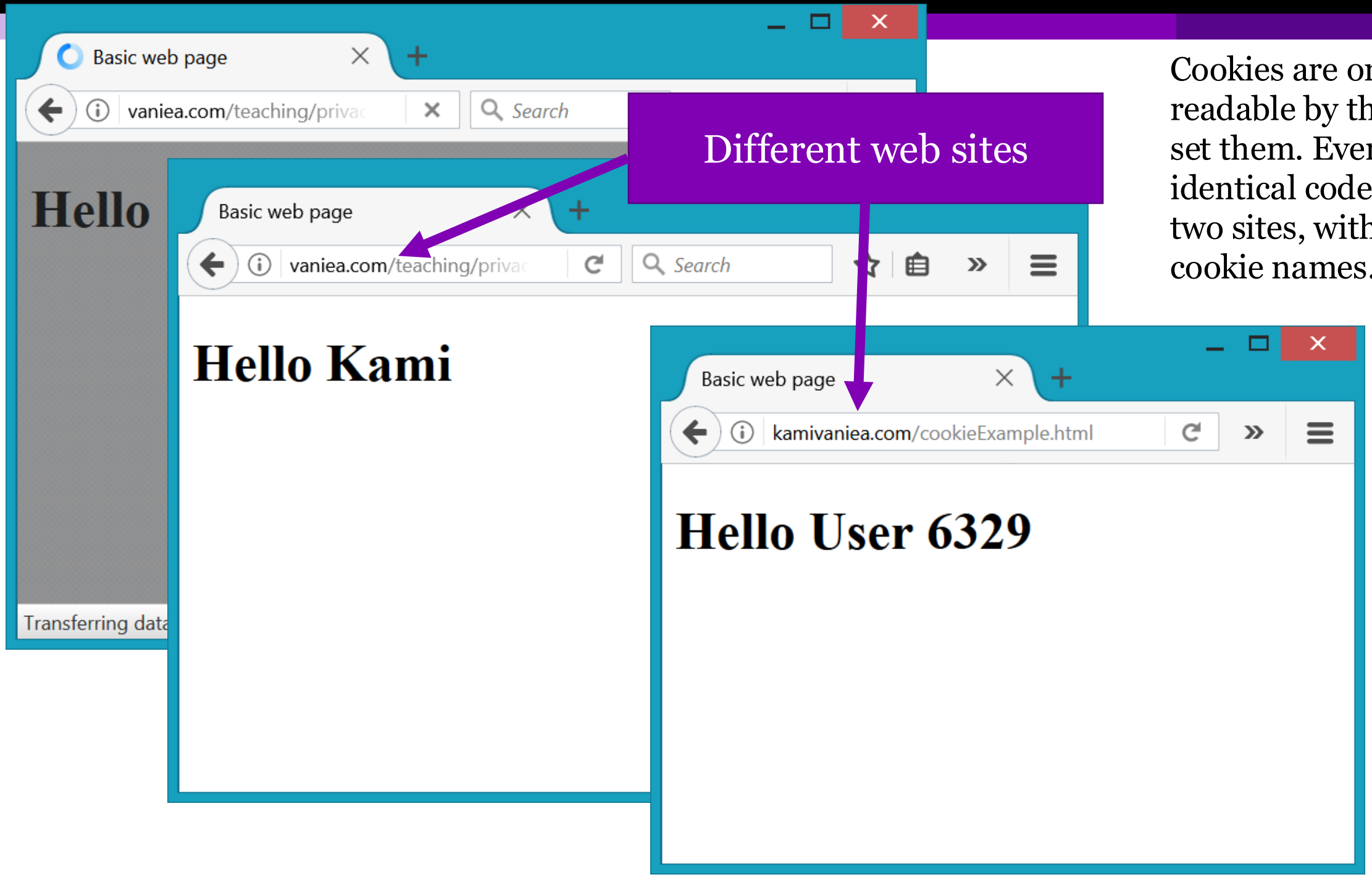
Loading cutedogs.com (fake site)



Think-pair-share

- Why are session cookies safe to use for security?

- Consider that:
  - A session cookie (random string) is used for continued authentication, even banks use it
  - Cookies can be read by Javascript
  - No login or other common authentication is needed to read cookies
  - Cookies are all stored in the same place in the computer



Cookies are only readable by the site that set them. Even if identical code is run on two sites, with identical cookie names.

Cookie setting policy

- A website/server can only set cookies for its own domain or the higher-level domain one level up. It cannot set for a subdomain other than its own.
- So vaniea.com can set/read cookies for:
  - vaniea.com
- Images.vaniea.com can set/read cookies for:
  - images.vaniea.com
  - vaniea.com
- Browsers forbid setting cookies for top level domains like .com or .co.uk

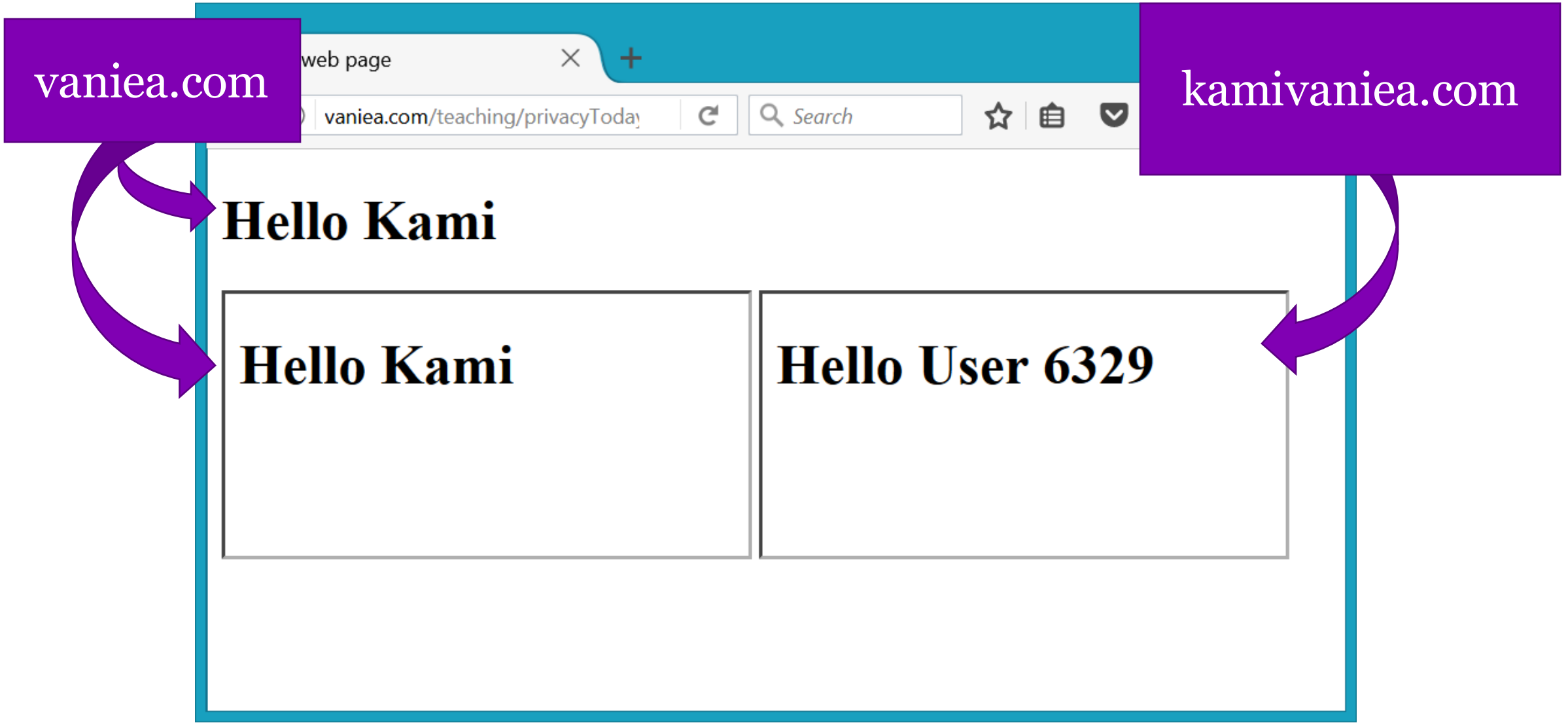
Remember Biba Integrity Model

- Focus on the integrity of the data rather than the confidentiality
- Subjects S and Objects O have Integrity values
- **Simple Integrity Property** – subjects at a given level of integrity must not read data at a lower integrity level (no read down)
- * **Integrity Property** – subjects at a given level of integrity must not write to data at a higher level of integrity (no write up)
- **Invocation Property** – processes from below cannot request higher access; only with subjects at an equal or lower level

While cookies are only shared with the site that set them. Multiple sites are contacted while building a website.

So if site A is being loaded by the browser, site B may be contacted to retrieve content. When site B is contacted all of site B's cookies are sent to B.

Two iframes reading and displaying two different cookies



Session cookies: two cookies set by UWaterloo Learn

Normal cookie

_gid:"GA1.2.1492176548.1720735134"
Created:"Thu, 11 Jul 2024 21:58:53 GMT"
Domain:".uwaterloo.ca"
Expires / Max-Age:"Sat, 13 Jul 2024 21:58:18 GMT"
HostOnly:false
HttpOnly:false
Last Accessed:"Fri, 12 Jul 2024 22:05:35 GMT"
Path:"/"
SameSite:"None"
Secure:false
Size:31

Session cookie

d2lSecureSessionVal:"lGdTkEvlO57vwd17wKDdtOH9Y"
Created:"Thu, 11 Jul 2024 21:58:50 GMT"
Domain:"learn.uwaterloo.ca"
Expires / Max-Age:"Session"
HostOnly:true
HttpOnly:true
Last Accessed:"Fri, 12 Jul 2024 22:05:35 GMT"
Path:"/"
SameSite:"None"
Secure:true
Size:44

Session cookies are a bit different

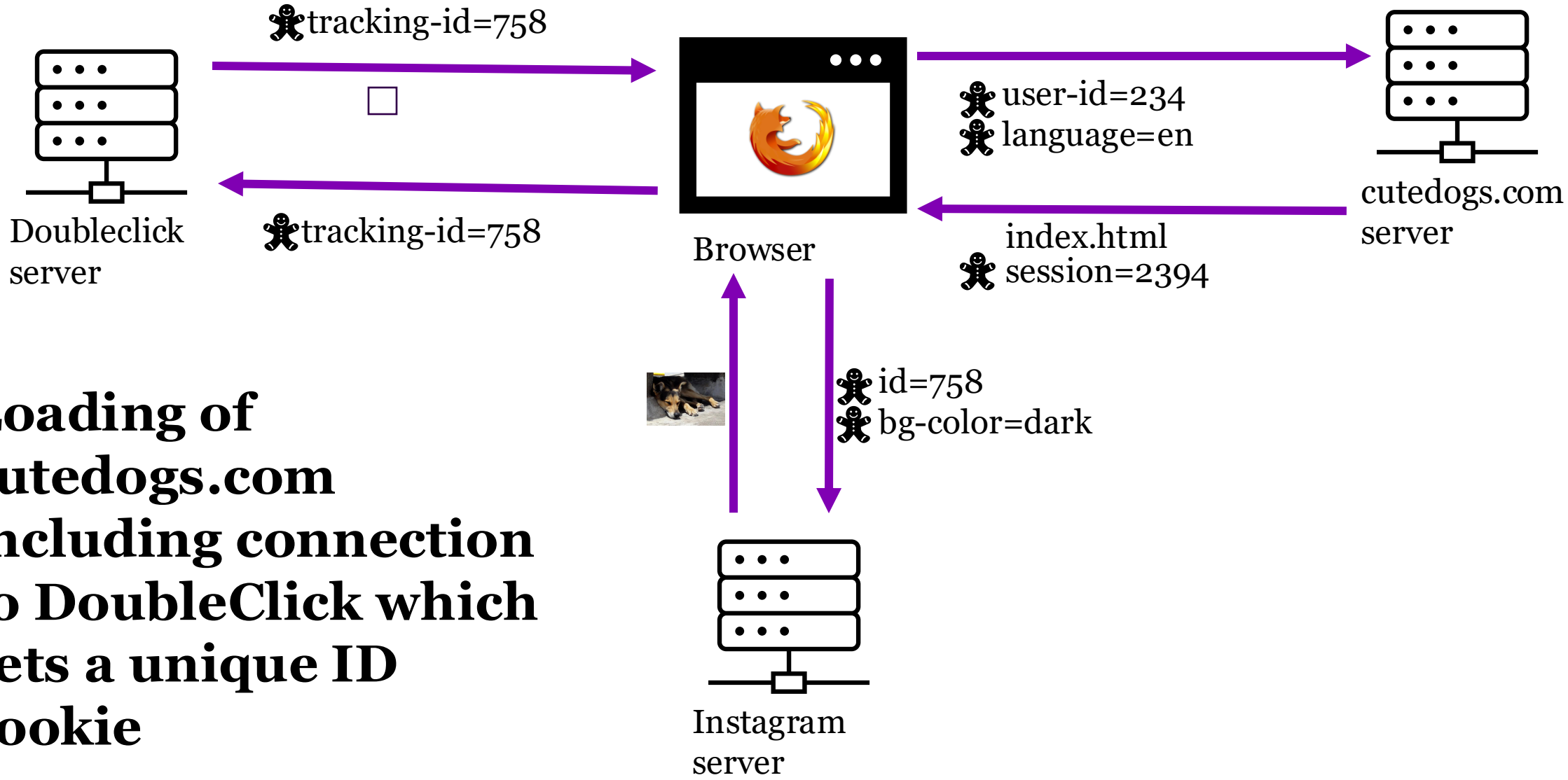
- Session cookies are just a normal cookie with no expiration
- Most browsers will delete expired or cookies without an expiration on browser restart
- Session cookies are meant to auto-delete after the end of a “session” where the web page is open
- Session cookies are considered less privacy-sensitive because they are not persistent

Session cookie

d2lSecureSessionVal:"lGdTkEvlO57vwd17wKDdtOH9Y"
Created:"Thu, 11 Jul 2024 21:58:50 GMT"
Domain:"learn.uwaterloo.ca"
Expires / Max-Age:"Session"
HostOnly:true
HttpOnly:true
Last Accessed:"Fri, 12 Jul 2024 22:05:35 GMT"
Path:"/"
SameSite:"None"
Secure:true
Size:44

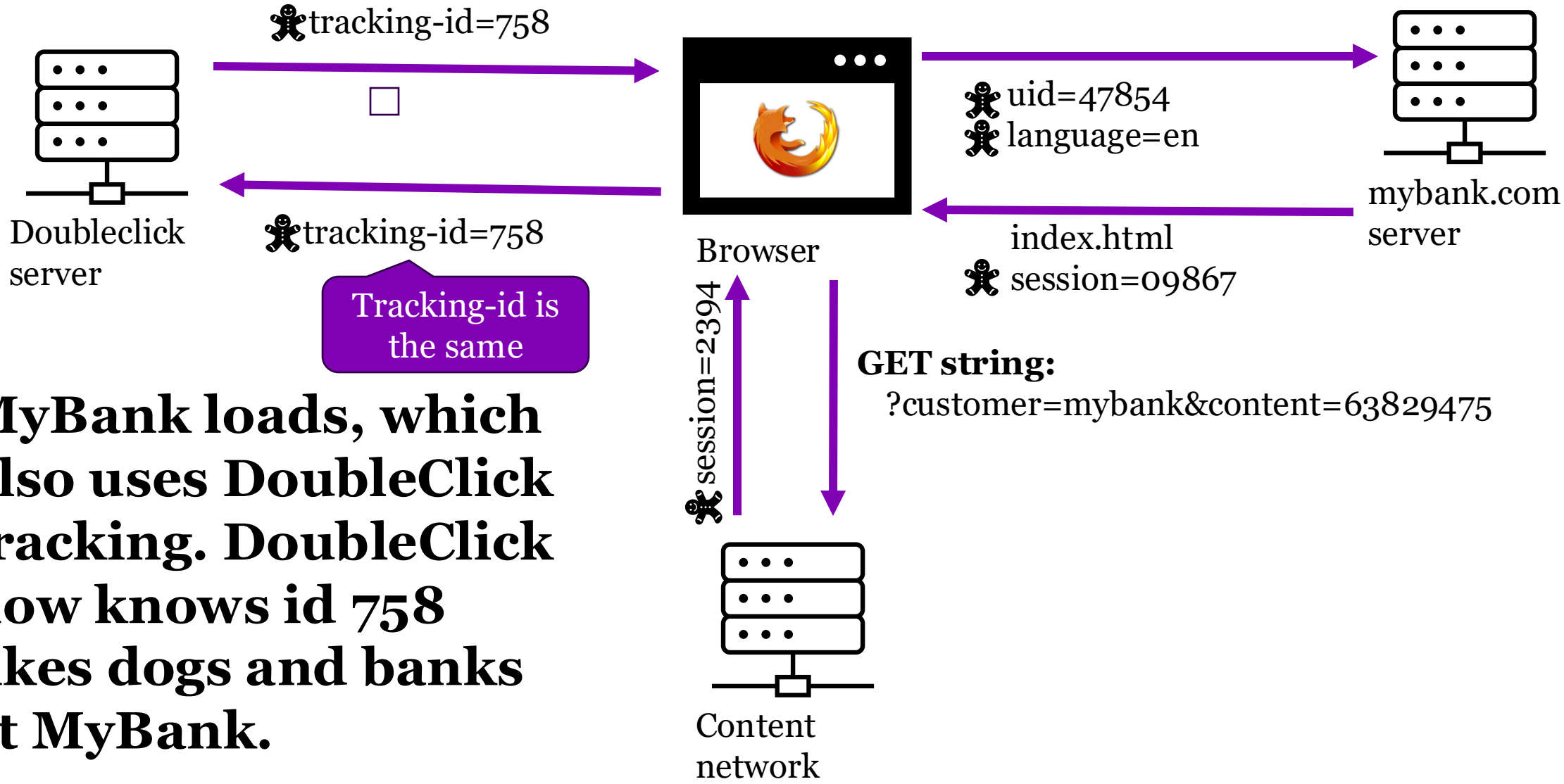
COOKIE-BASED PRIVACY ATTACKS

Tracking across the web

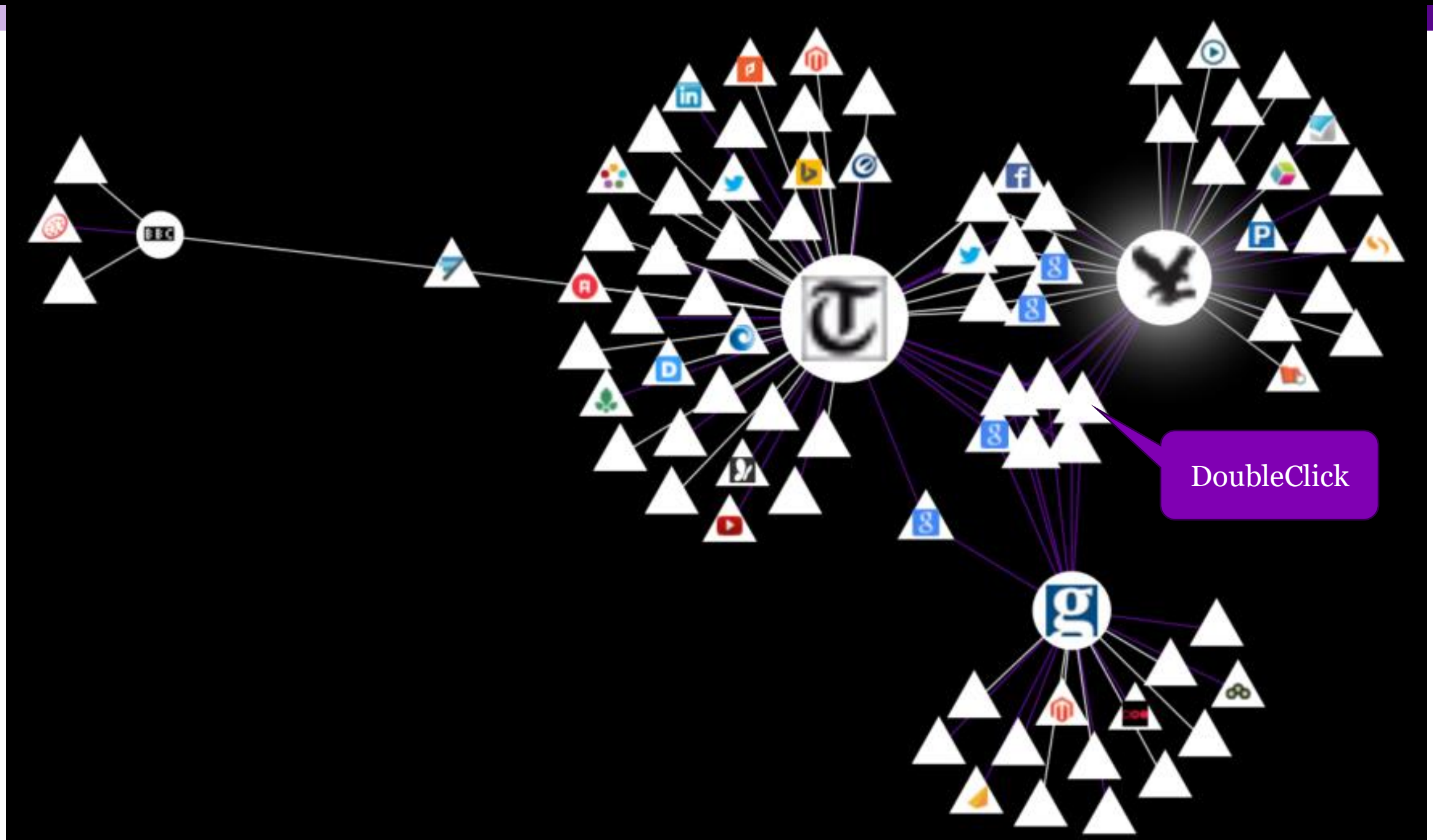


Loading of cutedogs.com including connection to DoubleClick which sets a unique ID cookie

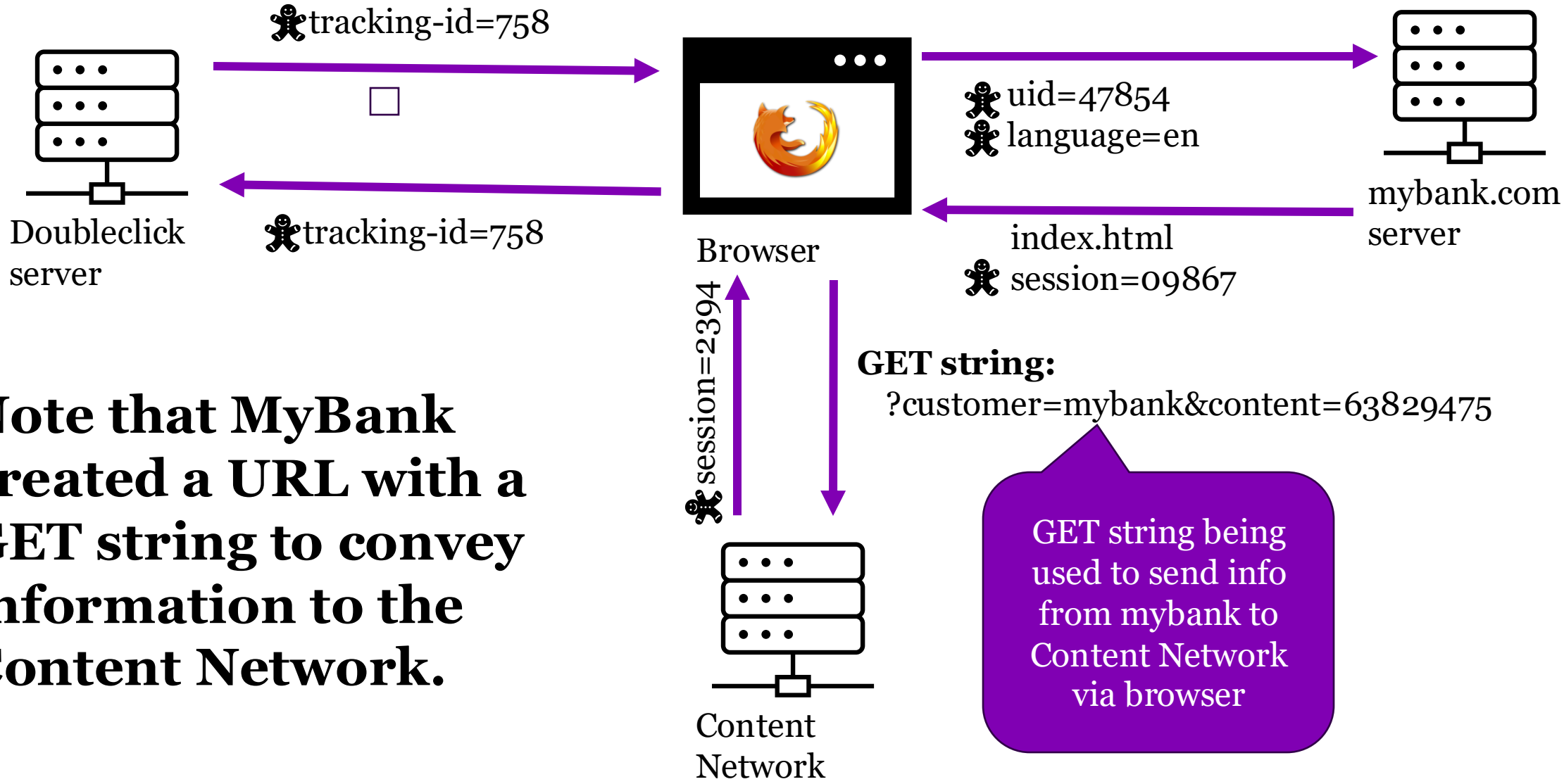
Tracking across the web



MyBank loads, which also uses DoubleClick tracking. DoubleClick now knows id 758 likes dogs and banks at MyBank.


DoubleClick

Tracking across the web



Note that MyBank created a URL with a GET string to convey information to the Content Network.

GET string used by main website to send information to other sites

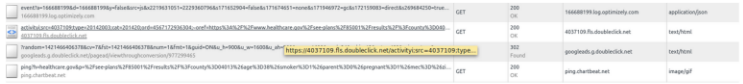
ELECTRONIC FRONTIER FOUNDATION

About Issues Our Work Take Action Too

HealthCare.gov Sends Personal Data to Dozens of Tracking Websites

BY COOPER QUINTIN | JANUARY 20, 2015

The Associated Press reports that healthcare.gov–the flagship site of the Affordable Care Act, where millions of Americans have signed up to receive health care–is quietly sending personal health information to a number of third party websites. The information being sent includes one's zip code, income level, smoking status, pregnancy status and more.



An example of personal health data being sent to third parties from healthcare.gov

EFF researchers have independently confirmed that healthcare.gov is sending personal health information to at least 14 third party domains, even if the user has enabled Do Not Track. The information is sent via the referrer header,

Discover more.

Email updates on news, actions, ev
area, and more.

Email Address

Postal Code (optional)

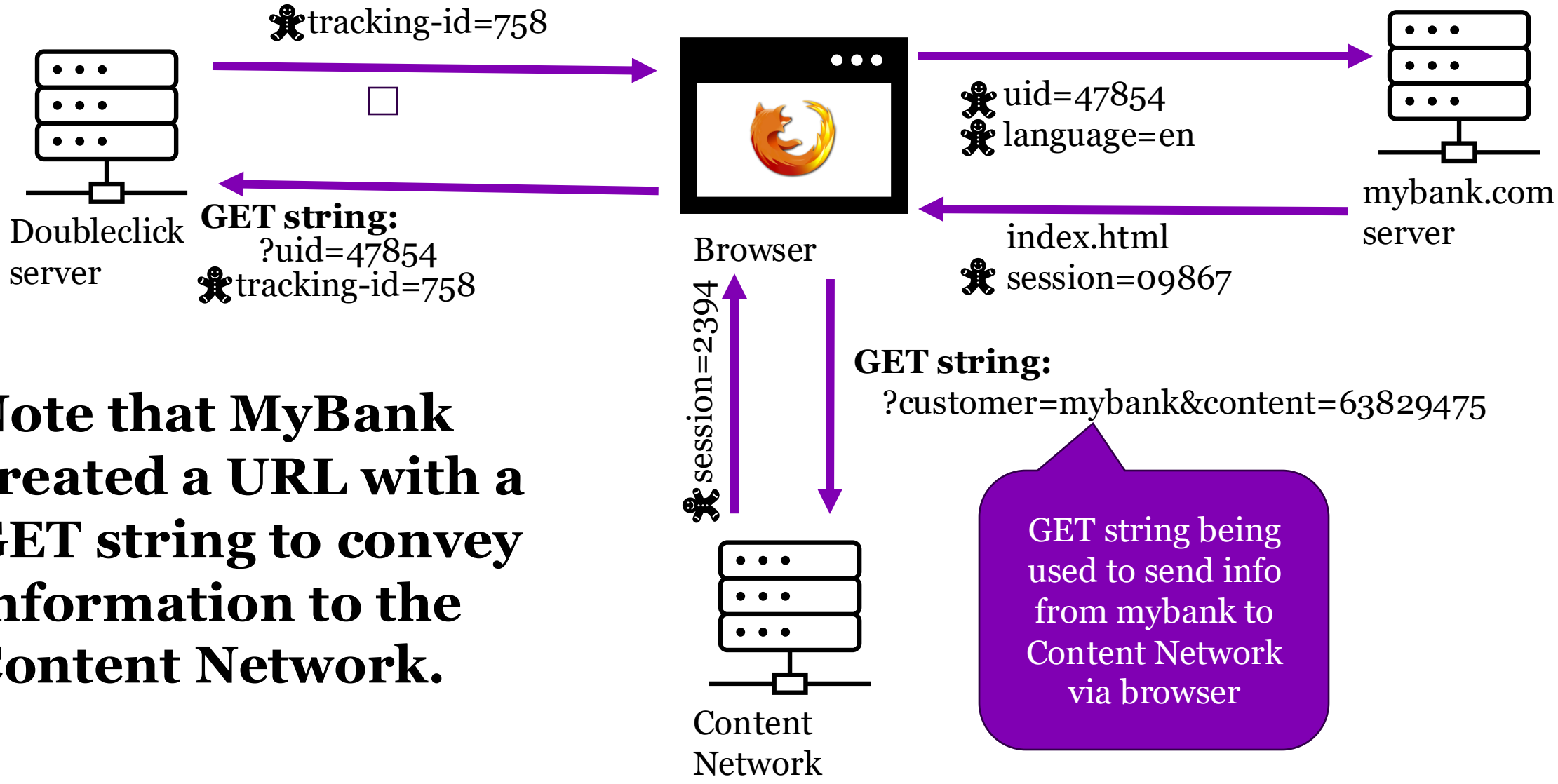
Anti-spam question: Enter the three-letter a
Electronic Frontier Foundation:

SUBMIT

https://4037109.fls.**doubleclick.net**/activityi;src=4037109;type=20142003;cat=201420;ord=7917385912018;~oref=https://www.healthcare.gov/see-plans/85601/results/?county=04019&**age=40&smoker=1&parent=&pregnant=1&mec=&zip=85601&state=AZ&income=35000&**&step=4?

&step=4?

Cookie syncing via GET string: put cookie content in GET



Note that MyBank created a URL with a GET string to convey information to the Content Network.

Verizon supercookie

- Verizon used a man-in-the-middle attack to inject a cookie into web requests from customers
- Other companies, like DoubleClick, could pay Verizon money to get details about the customers associated with each ID
- User was never informed
- No real way for a user to avoid a "supercookie" other than switching providers

FCC NEWS from the Federal Communications Commission

Media Contact:
Will Wiquist, (202) 418-0509
will.wiquist@fcc.gov

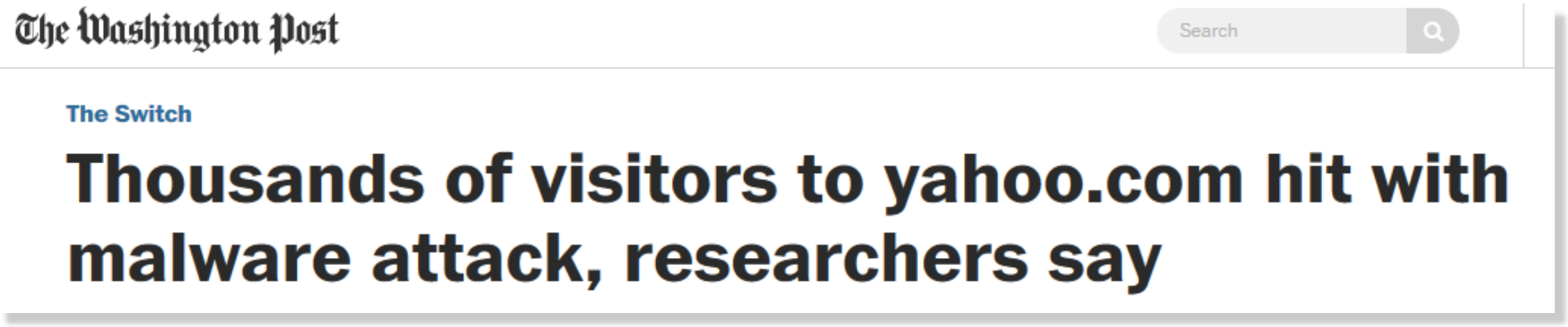
For Immediate Release

FCC SETTLES VERIZON "SUPERCOOKIE" PROBE, REQUIRES CONSUMER OPT-IN FOR THIRD PARTIES
Verizon Wireless to Obtain Affirmative Consent from Consumers Before Sending Unique Identifier Headers to Third Parties

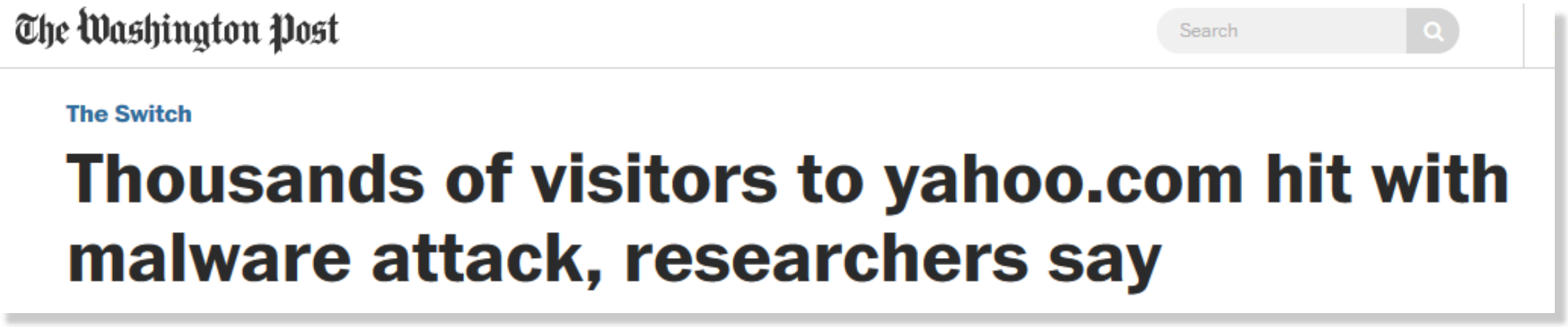
WASHINGTON, March 7, 2016 – The Federal Communications Commission today announced a settlement resolving an investigation into Verizon Wireless's practice of inserting unique identifier headers or so-called "supercookies" into its customers' mobile Internet traffic without their knowledge or consent. These unique, undeletable identifiers – referred to as UIDH – are inserted into web traffic and used to identify customers in order to deliver targeted ads from Verizon and other third parties. As a result of the investigation and settlement, Verizon Wireless is notifying consumers about its targeted advertising programs, will obtain customers' opt-in consent before sharing UIDH with third parties, and will obtain customers' opt-in or opt-out consent before sharing UIDH internally within the Verizon corporate family.

"Consumers care about privacy and should have a say in how their personal information is used, especially when it comes to who knows what they're doing online," said FCC Enforcement Bureau Chief Travis LeBlanc. "Privacy and innovation are not incompatible. This agreement shows that companies can offer meaningful transparency and consumer choice while at the same time continuing to innovate. We would like to acknowledge Verizon Wireless's cooperation during the course of this investigation and its willingness to make changes to its practices for the

3rd party content can be a source of malicious code.



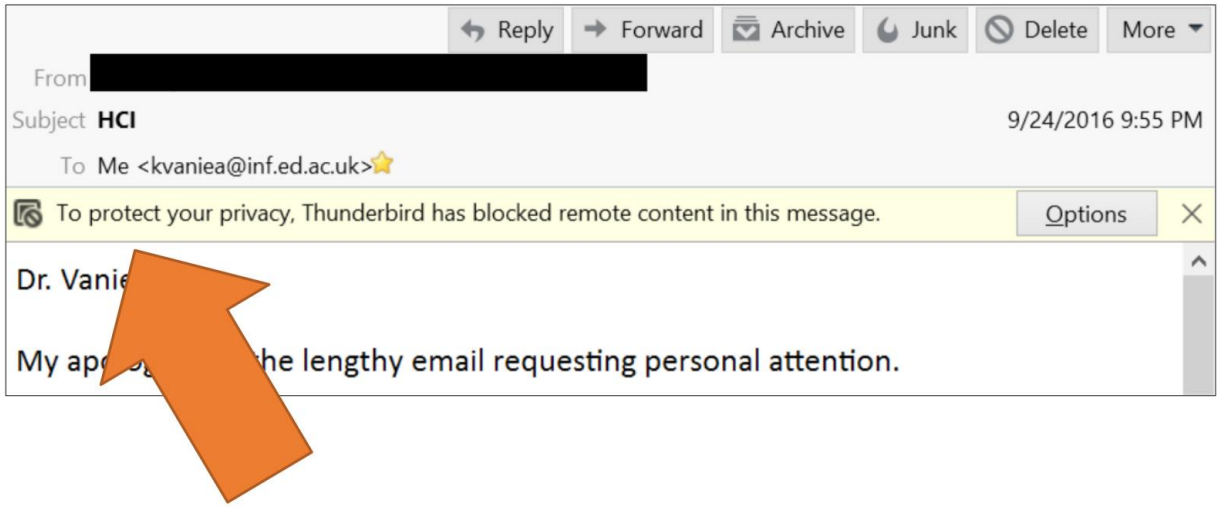
"Malicious payloads were being delivered to around 300,000 users per hour. The company guesses that around 9 percent of those, or 27,000 users per hour, were being infected."



Clients visiting yahoo.com received advertisements served by ads.yahoo.com. Some of the advertisements are malicious ... Instead of serving ordinary ads, the Yahoo's servers reportedly sends users an `exploit kit.

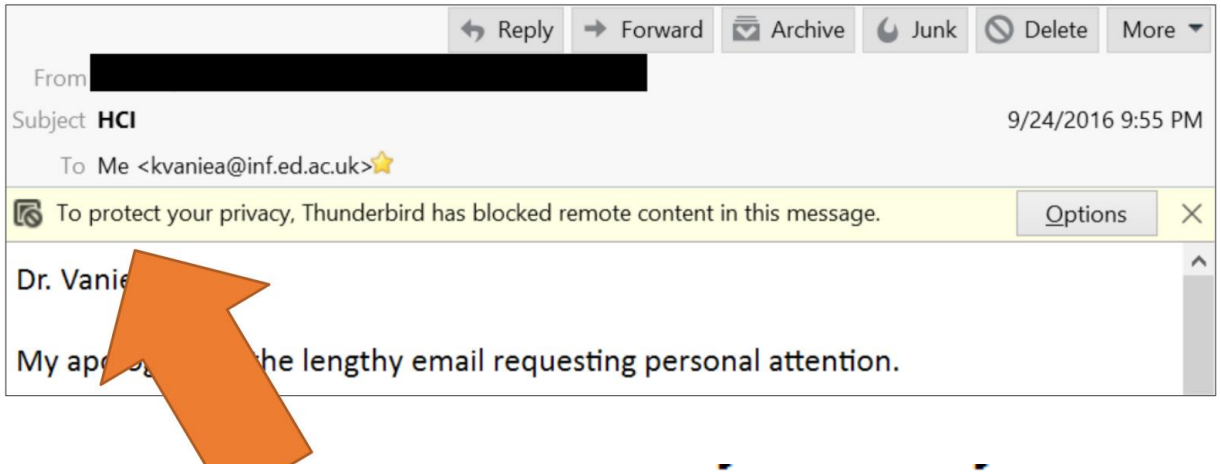
3rd party content can also be used for tracking.

Emails are similar to mini web pages, they load content the same way.



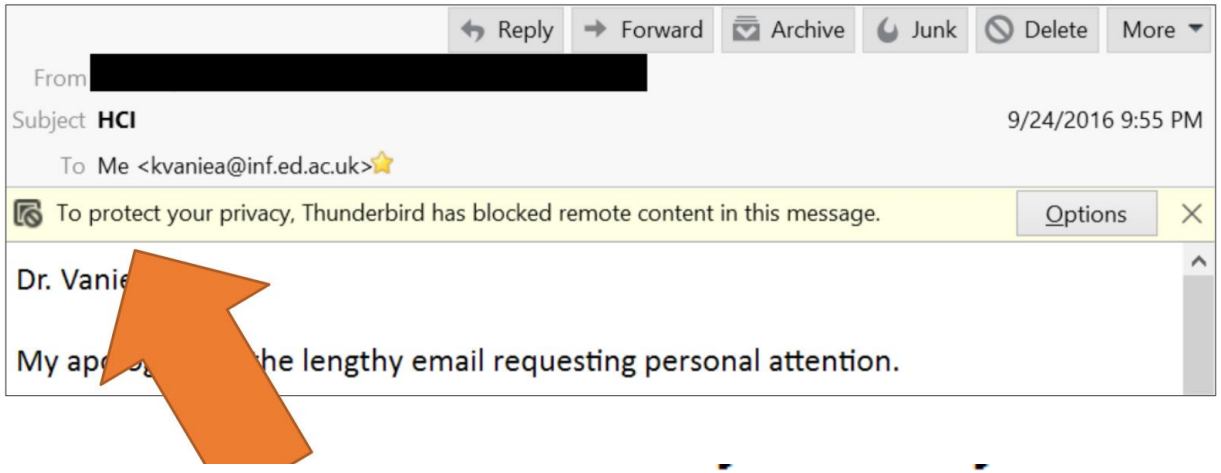
What is my email client warning me about?

Emails are similar to mini web pages, they load content the same way.




```
iv><div><br></div><div>Regards,</div><div>Chris</div></div><img src=3D"http=
://t.sidekickopen65.com/e1t/o/5/f18dQhb0S7ks8dDMPbW2n0x6l2B9gXrN7sKj6v4LGzz=
VQZptn64JsbFW3Lyy-Y2zlZNzW40Hqy21k1H6H0?si=3D6208290593964032&amp;pi=3D2ee4=
f8a0-67ac-43f0-cbe4-30cede291a88" style=3D"display:none!important" height=
=3D"1" width=3D"1"></div>
```

Emails are similar to mini web pages, they load content the same way.




```
iv><div><br></div><div>Regards,</div><div>Chris</div></div><img src=3D"http=
://t.sidekickopen65.com/e1t/o/5/f18dQhb0S7ks8dDMPbW2n0x6l2B9gXrN7sKj6v4LGzz=
VQZptn64JsbFW3Lyy-Y2zlZNzW40Hqy21k1H6H0?si=3D6208290593964032&amp;pi=3D2ee4=
f8a0-67ac-43f0-cbe4-30cede291a88" style=3D"display:none!important" height=
=3D"1" width=3D"1"></div>
```

The above code loads an invisible image (display:none) of size 1 pixel. Doing so causes your email client to ask for the image from the server, letting them know that you opened the email.

QUESTIONS