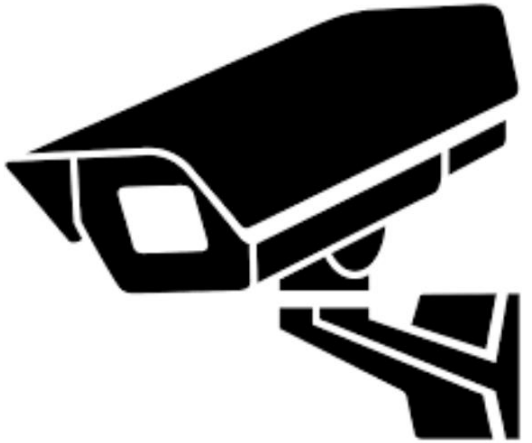


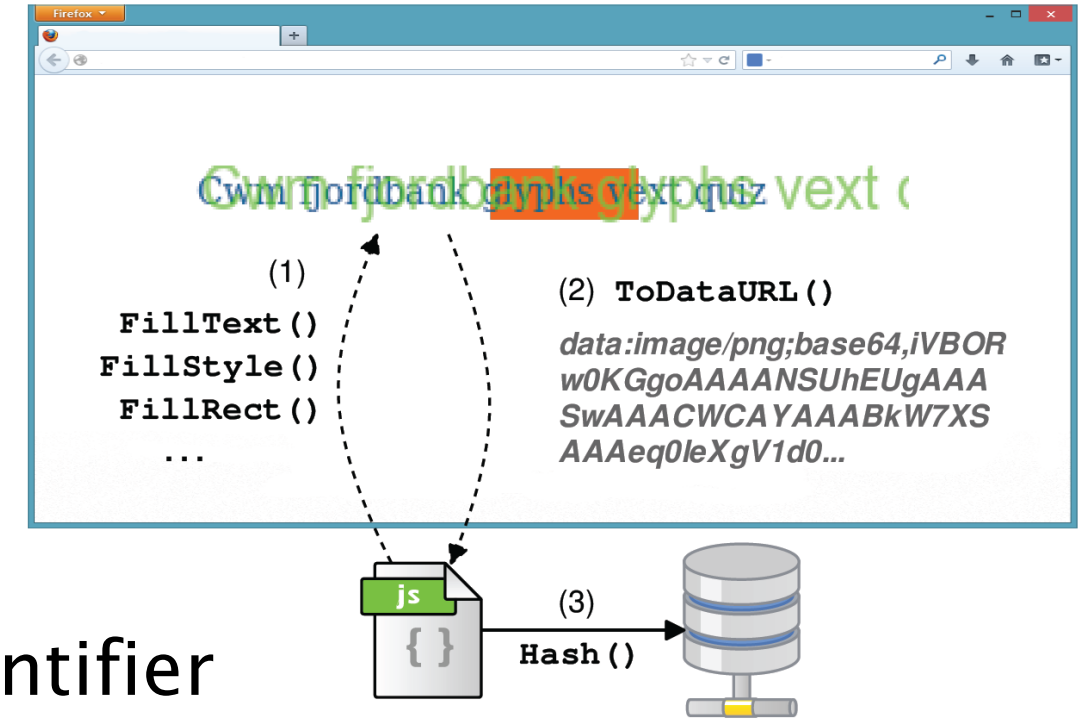
The web tracking arms race: past, present, and future

Arvind Narayanan

@random_walker

Canvas Fingerprinting: a sneaky tracking technique

1. Draw invisible text
2. Read it back as a sequence of bits



Tiny system differences

➔ Bit string acts as device identifier

Found it on over 5,500 sites out of top 100,000

Acar et al. *The Web Never Forgets: Persistent Tracking Mechanisms in the Wild.* ACM CCS 2014.

“Third party” online tracking

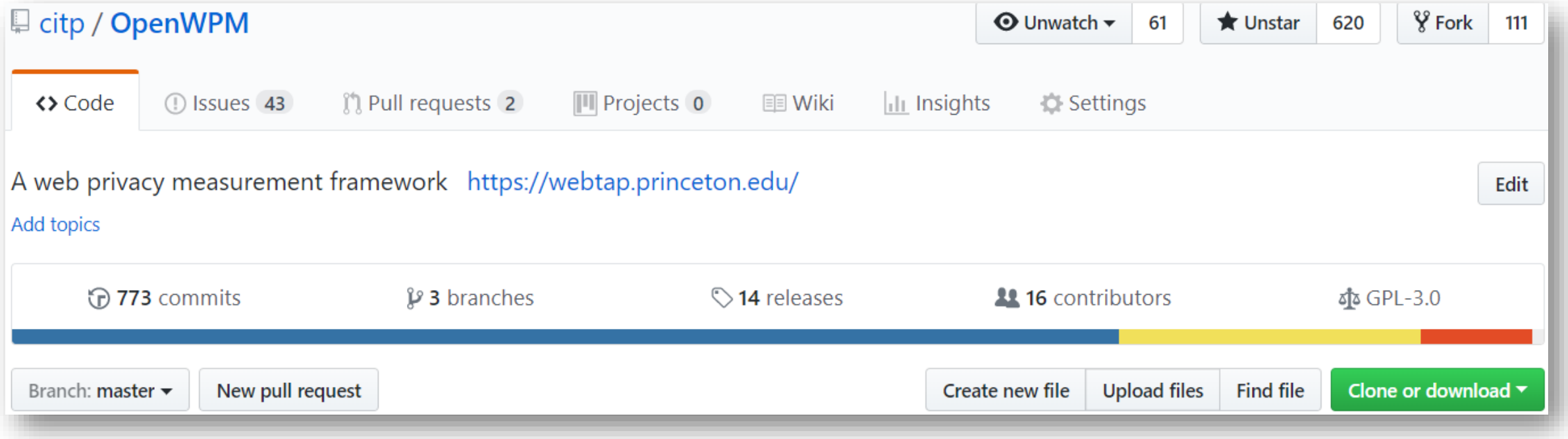
Sites other than the one you’re visiting

typically invisible

compiling profiles of your browsing history

What if oversight of online tracking could be *automated*?

OpenWPM is a mature, open-source tool

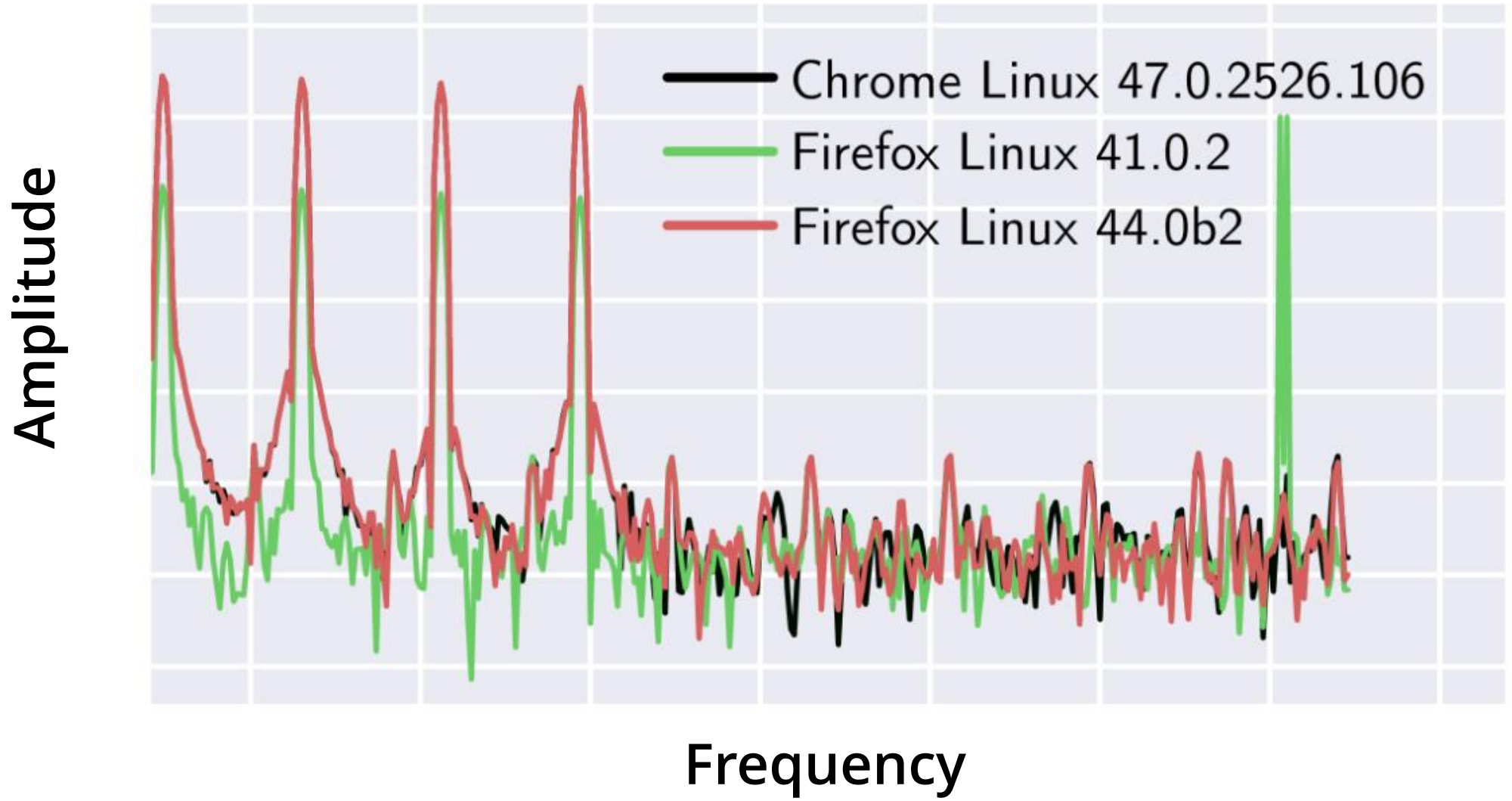


New types of fingerprinting

Audio, Battery, WebRTC APIs in HTML5 are all being abused by third-party scripts for fingerprinting

Englehardt & Narayanan. *Online tracking: a 1-million-site measurement and analysis*. CCS 2016.

Audio fingerprint

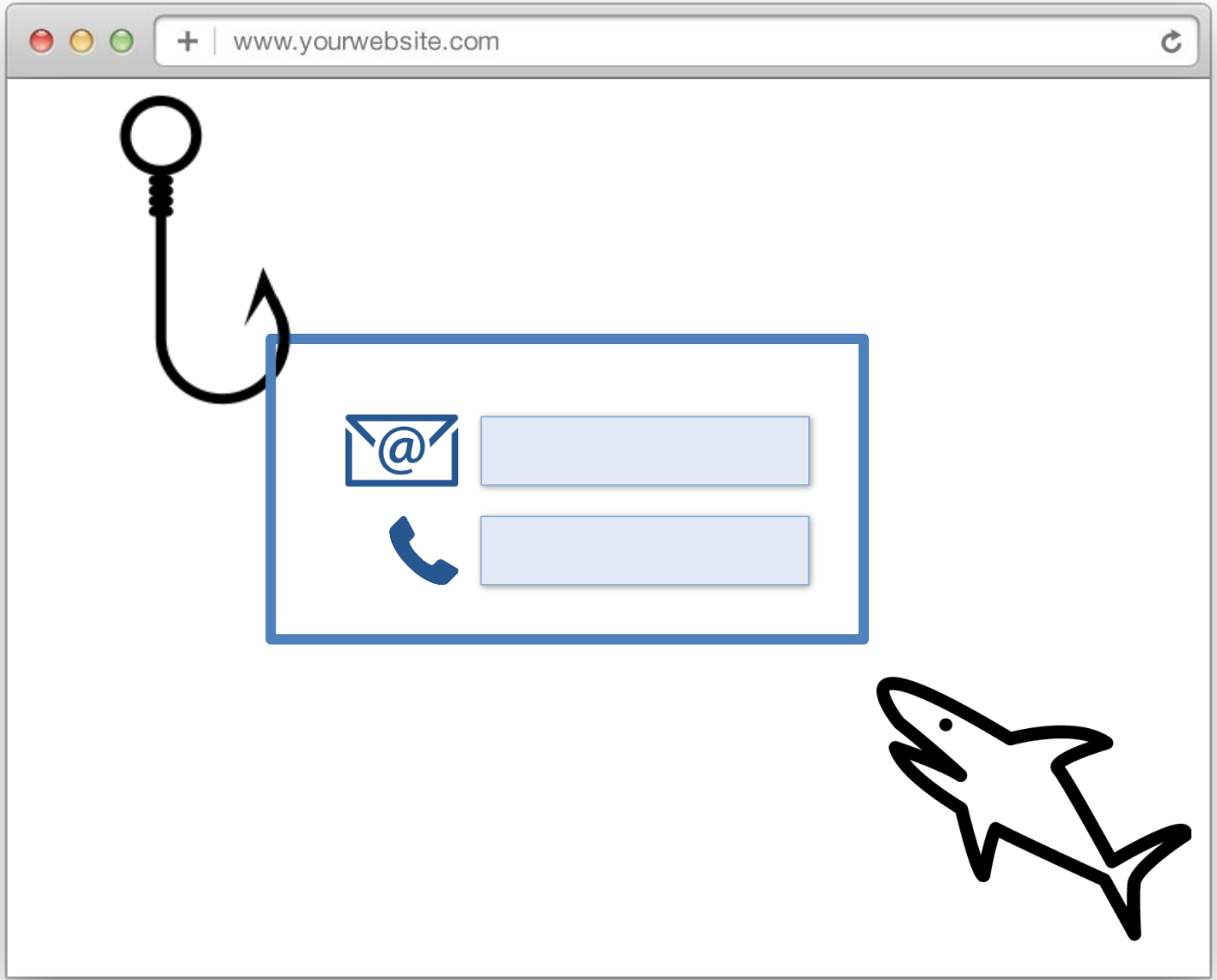


Isn’t it all anonymous?

Detecting PII exfiltration:

an information-flow problem

Detecting PII exfiltration: bait



Rampant exfiltration of PII by third parties

'Session replay' scripts record everything
(like someone looking over your shoulder)
and send it to a third party.

Includes passwords, medical info

Exfiltration happens even if form never submitted

Exfiltration confirmed on about 8,000 sites

HIPAA-protected (Walgreens) and FERPA-protected data (Gradescope)

Englehardt et al. *No boundaries: Exfiltration of personal data by session-replay scripts*.

Solutions

Regulation?


The cookie settings on this website are set to 'allow all cookies' to give you the very best experience. If you continue without changing these settings, you consent to this - but if you want, you can change your settings at any time **at the bottom of this page.**
Change settings
No, thanks
Find out more about Cookies >

Browser extensions?

Always playing catch-up

Tiny userbase

- Favors tech savvy users, exacerbates privacy divide

Poor privacy is a problem for democracy

The role of web browsers

Why haven’t browsers acted?

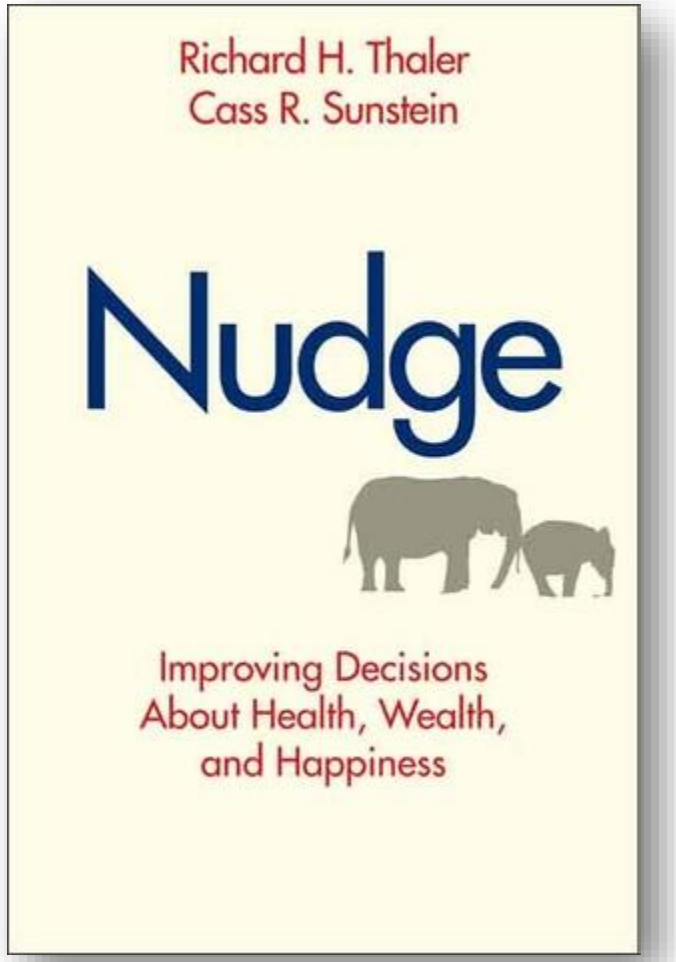
- Not traditionally seen as a security problem
- Attempt at neutrality

Browsers being neutral on third-party tracking

≈

Email providers being neutral on spam

Browser neutrality is not meaningful



Browser is a “choice architecture”

Trying to be neutral

➔ reifying historical accidents

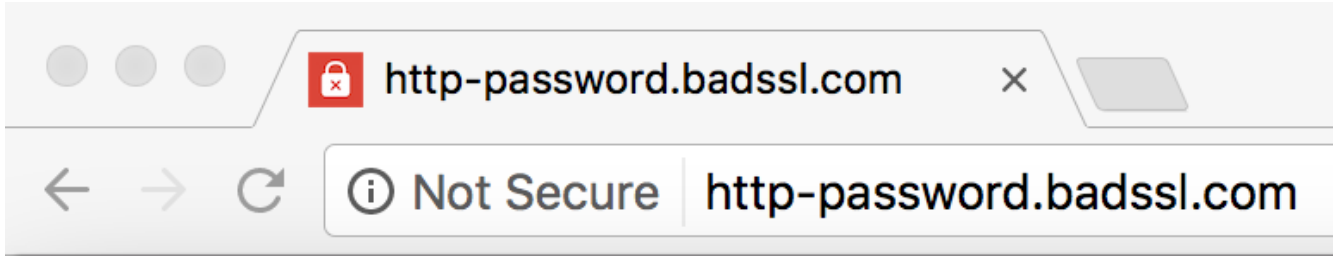
E.g. the web standard does <u>not</u> mandate that third-party cookies be silently allowed

“Neutrality” reinforces power imbalances

This has started to change

What could browser vendors do? Three ideas

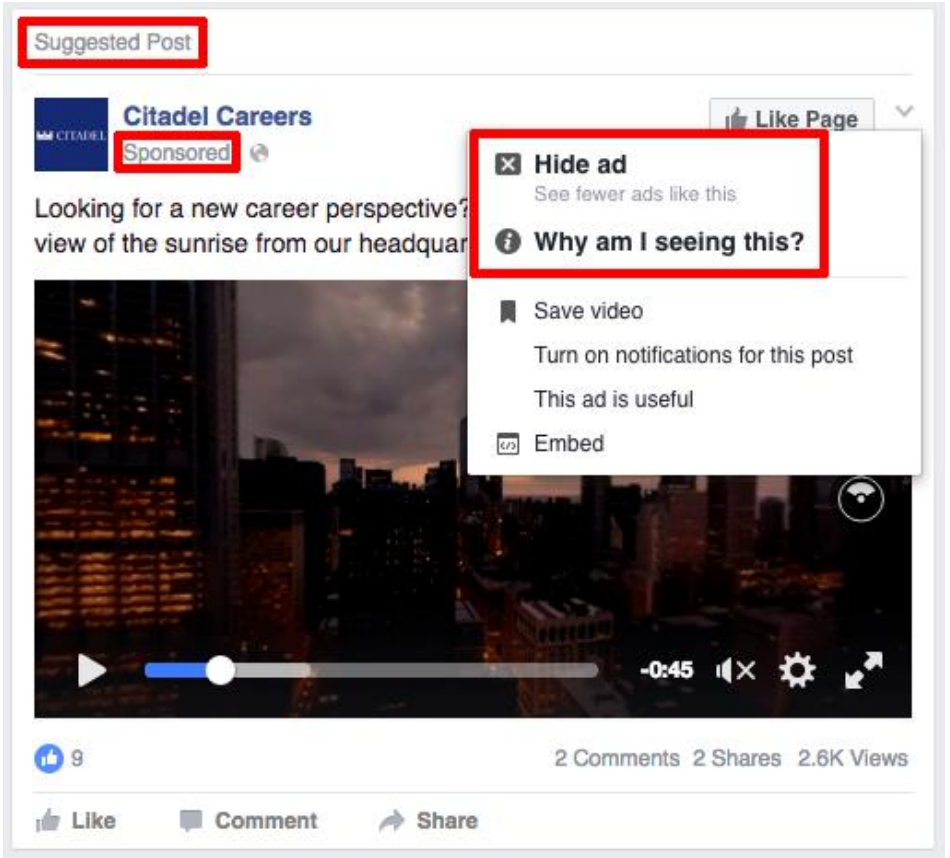
1. Publish clear policies on (un)acceptable tracking
2. Warn users when sites violate tracking policies



3. Create a tracking-protection mode analogous to private browsing mode

How far can we take this?

Perceptual ad blocker



Storey et al. *The future of ad blocking: An analytical framework and new techniques.*

The web is being used for engineering society

Browser vendors cannot avoid taking a side

Take-home message

The state of web privacy is a problem for society, not just for individuals

We have a collective moral responsibility to act

Browsers are **User-Agent**s
and should act in the interest of the user