CSE 484/M584: Computer Security (and Privacy)

Spring 2025

David Kohlbrenner
dkohlbre@cs

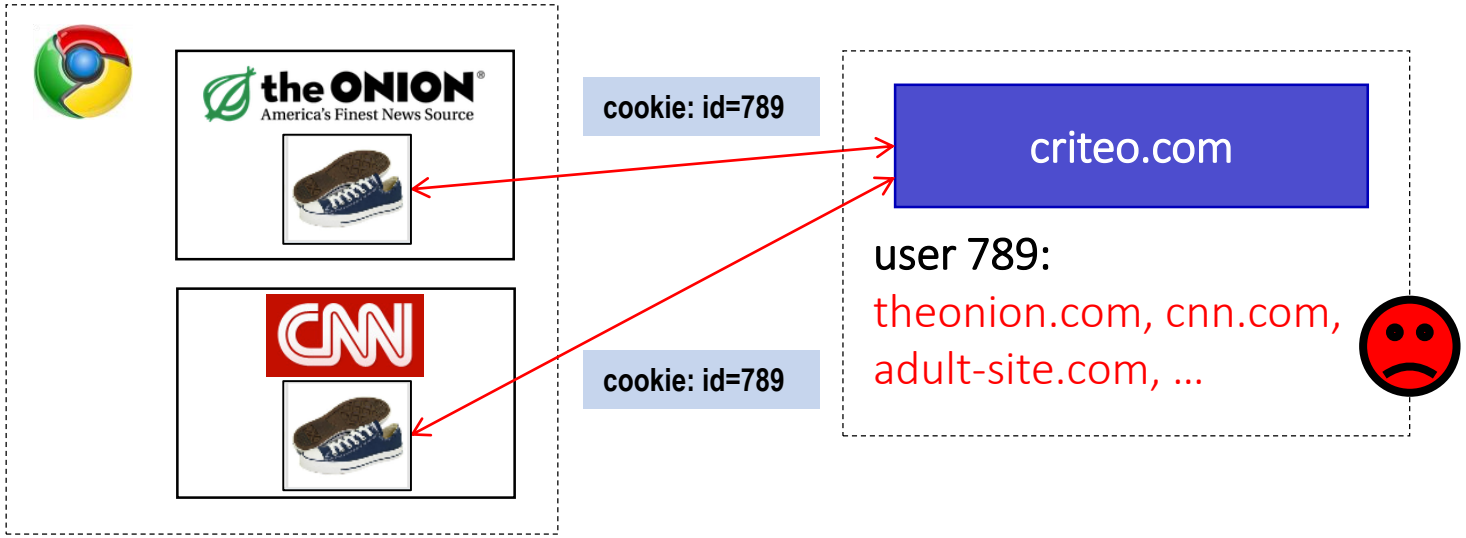
UW Instruction Team: David Kohlbrenner, Yoshi Kohno, Franziska Roesner, Nirvan Tyagi. Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials

Admin

- Lab 3 Weblab due next week.
  - Start early, etc etc

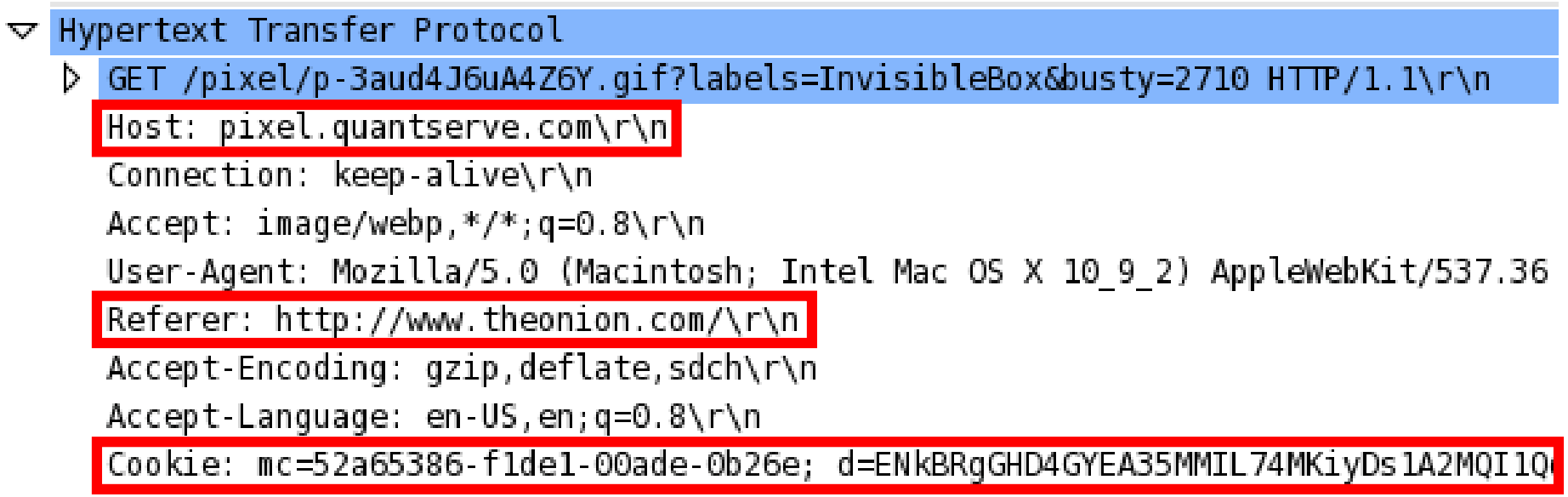
Anonymous Tracking

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.

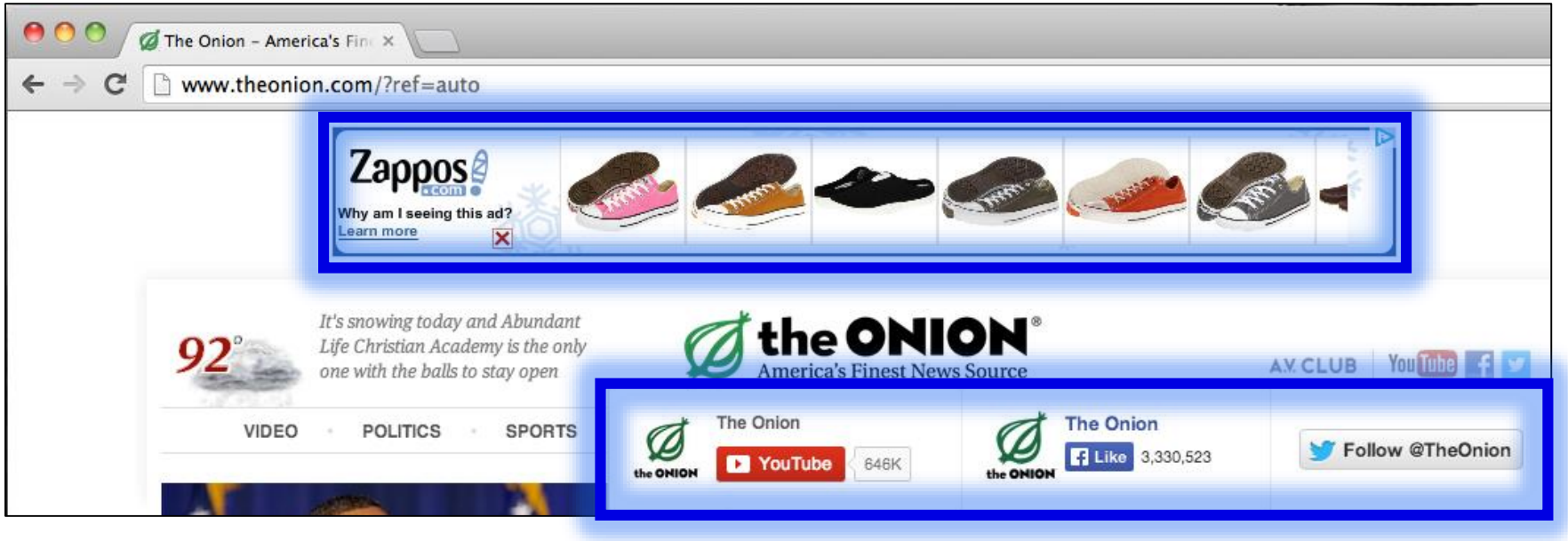


Tracking Technologies

- 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

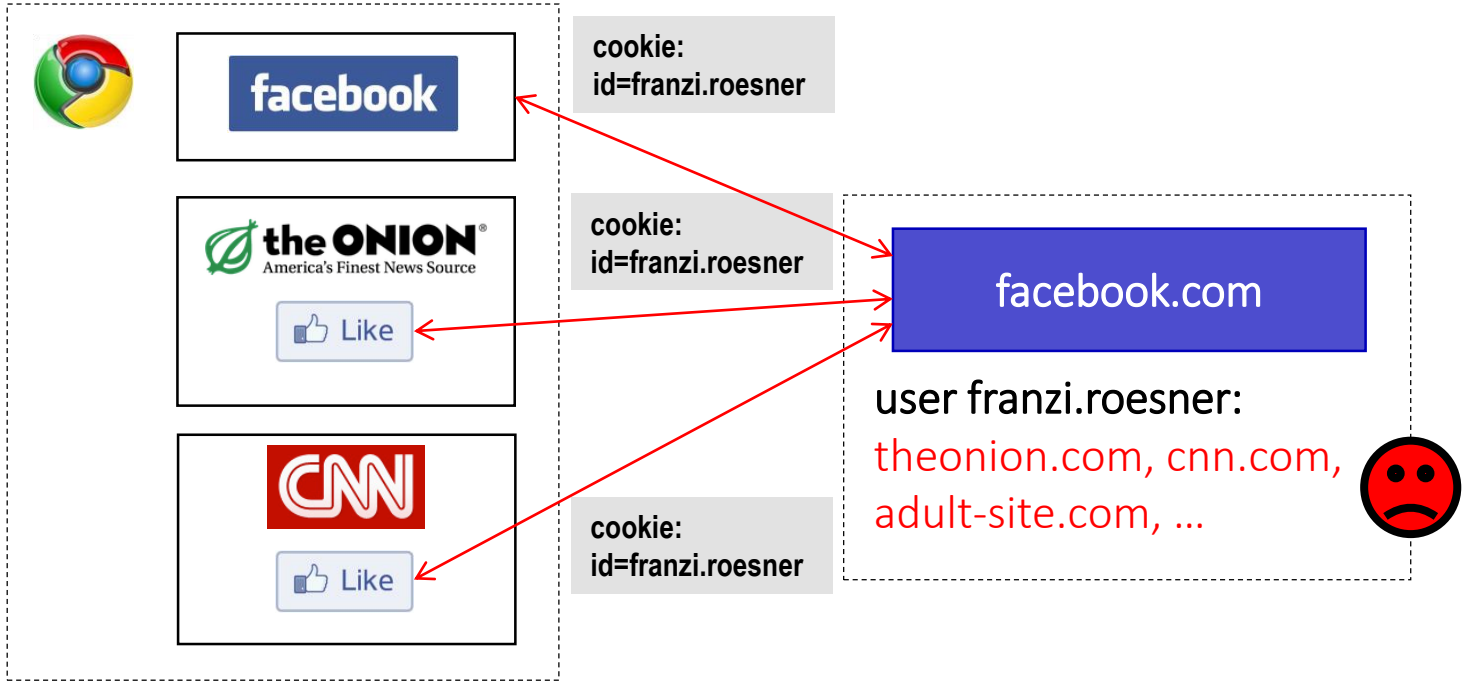
- "Zombie" cookies that respawn (http://samy.pl/evercookie)

Other Trackers?



"Personal" Trackers

Personal Tracking



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

Defenses to Reduce Tracking

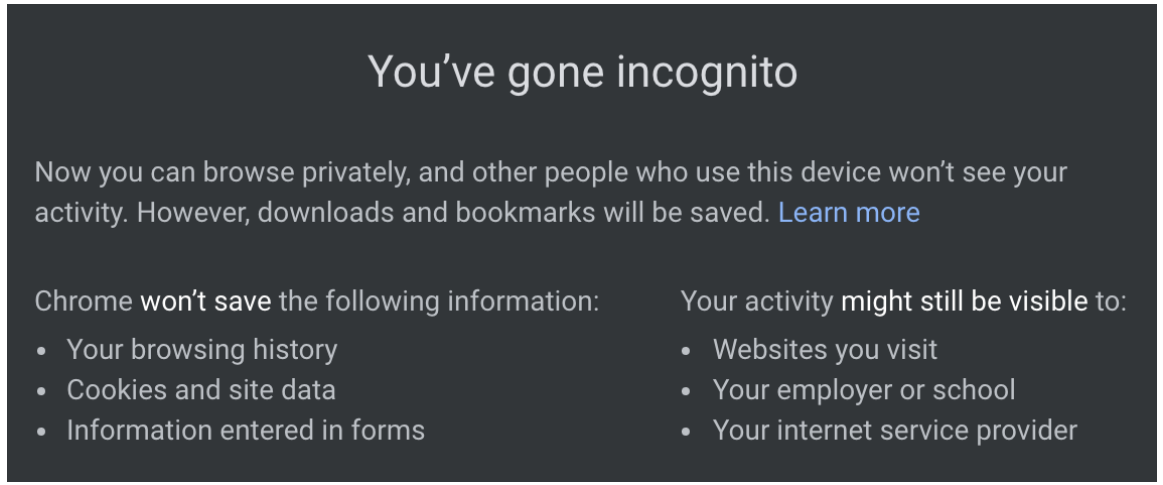
- Do Not Track?

Do Not Track is not a technical defense: trackers must honor the request.

Defenses to Reduce Tracking

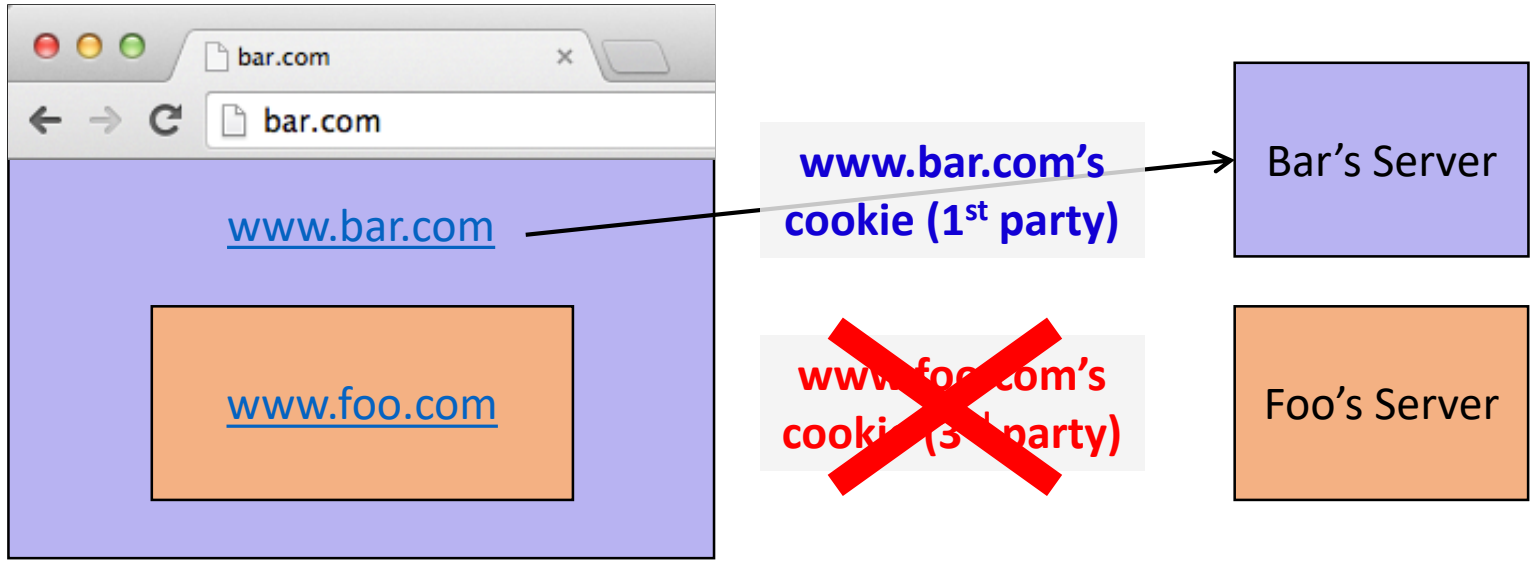
- Do Not Track proposal?
- Private browsing mode?

Private browsing mode doesn't protect against network attackers fully.



Defenses to Reduce Tracking

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



3rd party cookies

- Chrome…

> “By undermining the business model of many ad-supported websites, blunt approaches to cookies encourage the use of opaque techniques such as fingerprinting (an invasive workaround to replace cookies), which can actually reduce user privacy and control. We believe that we as a community can, and must, do better.”
>
> Aug 2022: Remove 3rd party cookies by 2024

The state of 3rd party cookies

- Safari:
  - Blocks most - https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/
- Chrome
  - No longer removing. https://privacysandbox.com/news/privacy-sandbox-next-steps/
- Firefox
  - Specific blocks/etc https://developer.mozilla.org/en-US/blog/goodbye-third-party-cookies/
- Others
  - Variety of behaviors, wide variation

https://www.cookiestatus.com/ -- vaguely up to date (2023)

Fingerprinting

- An alternative, popular, approach is *fingerprinting*
  - Website runs some javascript to measure browser/machine behavior
  - Generates an ID from this
  - ID is semi-consistent even across things like incognito mode

- Fingerprinting is unaffected by 3rd party cookie changes!

Gradescope: Fingerprint the browser!

- Your (ad company) goal is to track users whenever they load your <iframe>
- They don't have 3rd party cookies
- So you will measure their browser instead from JS.
- What might be a good thing to measure?

Fingerprinting

https://coveryourtracks.eff.org/about

- The user agent string from each browser
- The HTTP ACCEPT headers sent by the browser
- Screen resolution and color depth
- The Timezone your system is set to
- The browser extensions/plugins, like Quicktime, Flash, Java or Acrobat, that are installed in the browser, and the versions of those plugins
- The fonts installed on the computer, as reported by Flash or Java.
- Whether your browser executes JavaScript scripts

Fingerprinting

https://coveryourtracks.eff.org/about

- Yes/no information saying whether the browser accepts various kinds of cookies and "super cookies"
- A hash of the image generated by canvas fingerprinting
- A hash of the image generated by WebGL fingerprinting
- Yes/no whether your browser is sending the Do Not Track header
- Your system platform (e.g. Win32, Linux x86)
- Your system language (e.g. en-US)
- Your browser's touchscreen support

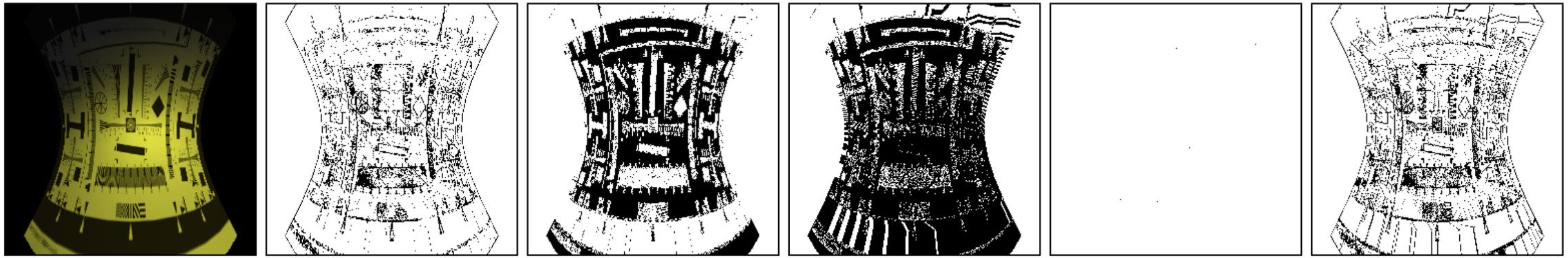
Fingerprinting

https://coveryourtracks.eff.org/about

- Yes/no information saying whether the browser accepts various kinds of cookies and "super cookies"
- **A hash of the image generated by canvas fingerprinting**
- **A hash of the image generated by WebGL fingerprinting**
- Yes/no whether your browser is sending the Do Not Track header
- Your system platform (e.g. Win32, Linux x86)
- Your system language (e.g. en-US)
- Your browser's touchscreen support

WebGL and Canvas Fingerprinting

- Every combination of OS, drivers, GPU, etc renders things *slightly differently.*
- This is deterministic.



(a) Original (Intel G41) (b) Group 1 (Radeon HD 2400) (c) Group 20 (Intel 82945G) (d) Group 23 (Intel G33/G31) (e) Group 25 (Intel HD Graphics) (f) Group 36 (GeForce 6200)

Figure 10: Original render and difference maps for Group 24

Pixel Perfect: Fingerprinting Canvas in HTML5, Keaton Mowery and Hovav Shacham (2012)

WebGL an

- Every combina ngs *slightly differently.*
- This is determi

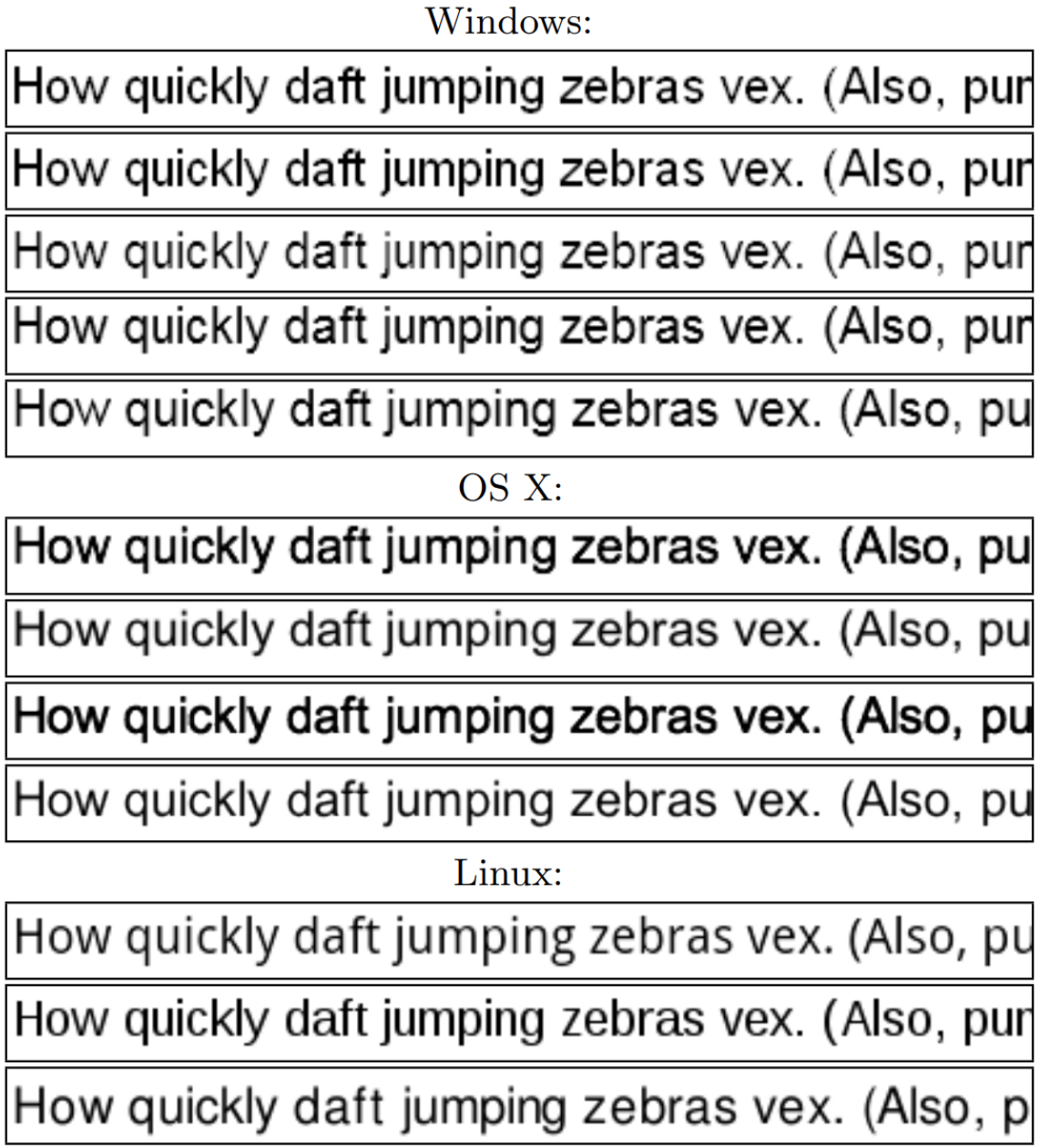


Figure 6: 13 ways to render 20px Arial

Pixel Perfect: F acham (2012)

Cookie ghostwriting

- No 3rd party cookies allowed ☹
- Instead, <script src=https://trackerdomain/cookiewriter.js/>
- No longer in an iframe… what can they do?

Journey to the Center of the Cookie Ecosystem: Unraveling Actors' Roles and Relationships, Sanchez-Rola et al.