CSCI-UA.9480
Introduction to Computer Security

Session 4.4
Web Privacy

Prof. Nadim Kobeissi

Web Privacy Goals

4.4a

Web privacy goals.

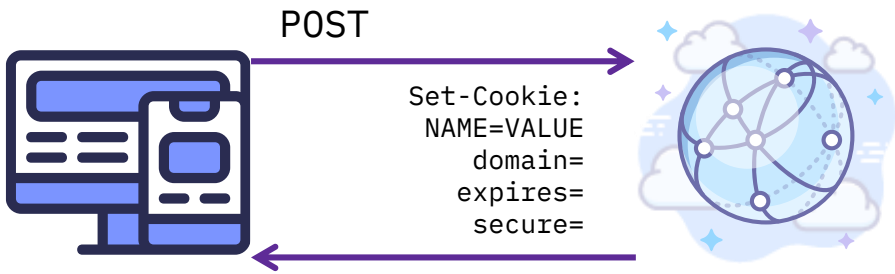
Preventing websites from learning:

- User identity.
- User behavior.
- Browsing behavior.
- Browser information.
- Location.
- IP address.

As seen previously: Cookies.

Cookies act as session identifiers or key-value stores between the web client and web server.

- Once the client logs in, the server may issue them a secret *session cookie* that they both then keep track of.
- *Secure cookies* are sent only over HTTPS.
- *httpOnly cookies* can be sent over HTTP or HTTPS (misleading name) but cannot be accessed by JavaScript via `document.cookies`.



Cookies can be used for tracking, too.

- Store unique tracking identifier.
- Use it to monitor user across the Internet, update your model of their behavior, etc.

Example:

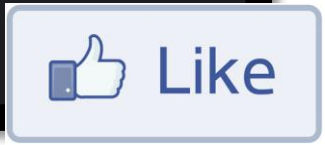
- Facebook's "Like" button allows it to monitor people across the entire Internet even when they're not logged into Facebook, by setting cookies and injecting JS code.

```
<html>
<head>
  <title>Your Website Title</title>
    <!-- You can use open graph tags to customize link previews.
    Learn more: https://developers.facebook.com/docs/sharing/webmasters -->
  <meta property="og:url"           content="https://www.your-domain.com/your-page.html" />
  <meta property="og:type"          content="website" />
  <meta property="og:title"         content="Your Website Title" />
  <meta property="og:description"   content="Your description" />
  <meta property="og:image"         content="https://www.your-domain.com/path/image.jpg" />
</head>
<body>

  <!-- Load Facebook SDK for JavaScript -->
  <div id="fb-root"></div>
  <script>(function(d, s, id) {
    var js, fjs = d.getElementsByTagName(s)[0];
    if (d.getElementById(id)) return;
    js = d.createElement(s); js.id = id;
    js.src = "https://connect.facebook.net/en_US/sdk.js#xfbml=1&version=v3.0";
    fjs.parentNode.insertBefore(js, fjs);
  }(document, 'script', 'facebook-jssdk'));</script>

  <!-- Your like button code -->
  <div class="fb-like"
    data-href="https://www.your-domain.com/your-page.html"
    data-layout="standard"
    data-action="like"
    data-show-faces="true">
  </div>

</body>
</html>
```

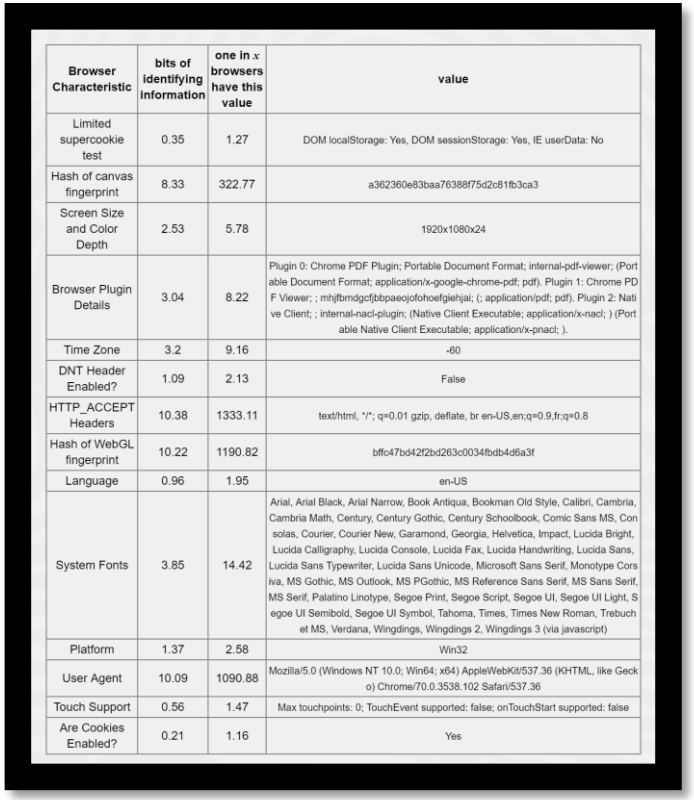


Panopticlick: test out browser fingerprinting.

A “browser fingerprint” can be created by aggregating information about your browser.

- Screen size.
- Time zone.
- Available system fonts.
- Cookies.
- Language.
- Etc.

Let’s try it out! https://panopticlick.eff.org/



Browser Characteristic	bits of identifying information	one in x browsers have this value	value
Limited supercookie test	0.35	1.27	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No
Hash of canvas fingerprint	8.33	322.77	a362360e83baa76388f75d2c81fb3ca3
Screen Size and Color Depth	2.53	5.78	1920x1080x24
Browser Plugin Details	3.04	8.22	Plugin 0: Chrome PDF Plugin; Portable Document Format; internal-pdf-viewer; (Portable Document Format; application/x-google-chrome-pdf; pdf). Plugin 1: Chrome PDF Viewer; ; mhjfbmdgcfjbbpaeojofohoefgiehjai; (; application/pdf; pdf). Plugin 2: Native Client; ; internal-nacl-plugin; (Native Client Executable; application/x-nacl;) (Portable Native Client Executable; application/x-pnacl;).
Time Zone	3.2	9.16	-60
DNT Header Enabled?	1.09	2.13	False
HTTP_ACCEPT Headers	10.38	1333.11	text/html, */*; q=0.01 gzip, deflate, br en-US,en;q=0.9,fr;q=0.8
Hash of WebGL fingerprint	10.22	1190.82	bffc47bd42f2bd263c0034fbdb4d6a3f
Language	0.96	1.95	en-US
System Fonts	3.85	14.42	Arial, Arial Black, Arial Narrow, Book Antiqua, Bookman Old Style, Calibri, Cambria, Cambria Math, Century, Century Gothic, Century Schoolbook, Comic Sans MS, Consolas, Courier, Courier New, Garamond, Georgia, Helvetica, Impact, Lucida Bright, Lucida Calligraphy, Lucida Console, Lucida Fax, Lucida Handwriting, Lucida Sans, Lucida Sans Typewriter, Lucida Sans Unicode, Microsoft Sans Serif, Monotype Corsiva, MS Gothic, MS Outlook, MS PGothic, MS Reference Sans Serif, MS Sans Serif, MS Serif, Palatino Linotype, Segoe Print, Segoe Script, Segoe UI, Segoe UI Light, Segoe UI Semibold, Segoe UI Symbol, Tahoma, Times, Times New Roman, Trebuchet MS, Verdana, Wingdings, Wingdings 2, Wingdings 3 (via javascript)
Platform	1.37	2.58	Win32
User Agent	10.09	1090.88	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Touch Support	0.56	1.47	Max touchpoints: 0; TouchEvent supported: false; onTouchStart supported: false
Are Cookies Enabled?	0.21	1.16	Yes

Web Privacy Tools

4.4b

Privacy Badger: blocks invisible trackers.

A “browser fingerprint” can be created by aggregating information about your browser.

- Screen size.
- Time zone.
- Available system fonts.
- Cookies.
- Language.
- Etc.

https://www.eff.org/privacybadger/

HTTPS Everywhere.

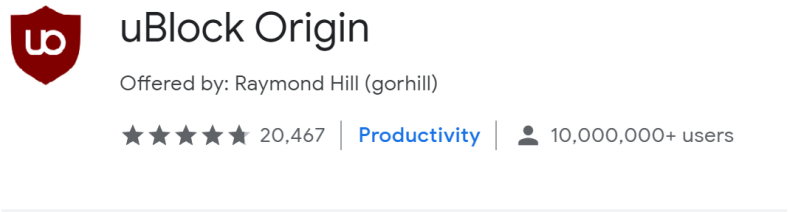
Uses a list of rules to translate HTTP addresses to HTTPS.

https://www.eff.org/https-everywhere

Ad blockers: Ublock origin.

- Use lists to block ads, trackers, even malware.
- Also makes browsing nicer.
- Debatable ethical implications (“acceptable ads” a potential solution?)

Note: Ublock origin is different from “Ublock”.



Recent legal tools: Europe's GDPR.

Enforces many requirements on services:

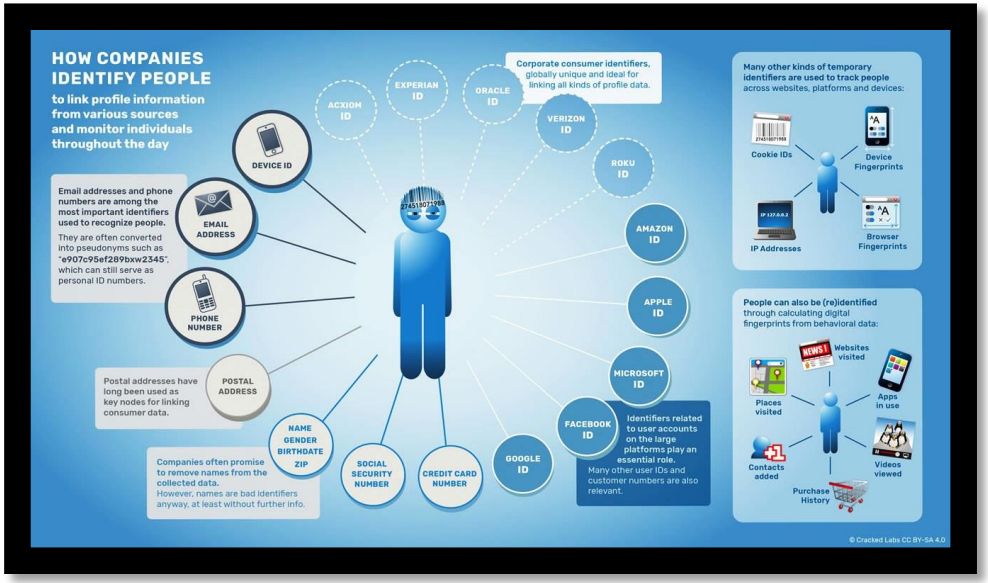
- Anonymization and/or encryption of personal data.
- Ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data.
- Ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident.
- Process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Recent legal tools: Europe's GDPR.

Companies must be clear about how *all* personal data is treated, stored, communicated.

Especially important in today's world, where tracking is used to shake up elections, etc.

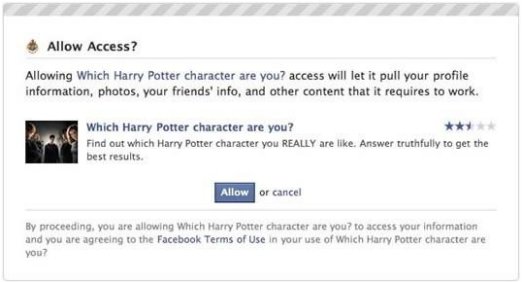
But is it enough? Is it even relevant?

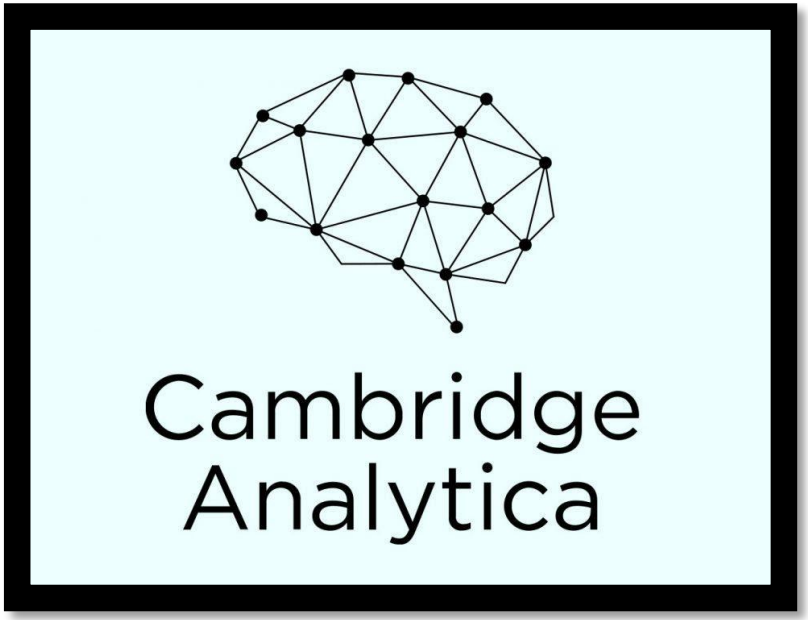


Motivating example: Cambridge Analytica.

More about this at December 3rd event!

- Harvested Facebook profile data through the permission dialogues people consented to for access to personality quizzes and the like (“Which Harry Potter Character Are You?”) etc.





Next time: Spam and Abuse

4.5