LEARN WEB

ale66

github.com/ale66/learn-web

WEB PRIVACY

DATA COLLECTION AND PRIVACY ISSUES

Leave Ethical considerations aside to examine what can be technically collected and how to avoid it

Currently, it is believed that Google et al. collect

- device information
- IP address -> geolocation
- usage of Google services: YT, Gmail, Gmaps…
- which ads one clicks and their location on the page
- more identifying info. from *partner* services

all such data may be used for targeted/re-targeted *ad placement* and *search relevancy*

Data can be purchased by third-parties via

- Google Analytics.
- FB for business/CrowdTangle

THIRD-PARTY TRACKERS

According to the EFF foundation:

“When you visit a webpage parts of the page may come from domains and servers other than the one you asked to visit

This is an essential feature of hypertext

On the modern Web, embedded images and code often use cookies and other methods to track your browsing habits — often to display advertisements

The domains that do this are called third party trackers“

LOGICAL FALLACIES

Saying *‘I don’t have anything to hide’*

customer profiling and tracking is never neutral and hardly positive

While it promises to customise advertisement so that it’s relevant to the user, the fact that such data exists is dangerous in itself and invites abuse

Alt. approach: use photos of AI-generated non-persons

END-TO-END ENCRYPTION

Becoming a standard today, it purports to eliminate *eavesdropping* and *impersonation*

In principle, it prevents potential eavesdroppers – including telecom providers, Internet providers, and even the provider of the communication service – from being able to access the cryptographic keys needed to decrypt the conversation

Wikipedia

ENCRYPTION, CONT'D

Seen as an extension of mail privacy rights, it does much more

It is based on notions of Number theory (requires finding the prime factors of large integers)

decryption takes practically forever

NO EXCHANGE OF SECRETS

Each participant will have a pair of keys: one public and one private not for sharing

Its development provides the basis of crypto-currencies

While probably based on a *paranoid* vision of liberal societies, E2E encryption helps in many instances

INCOGNITO PAGES

browsers will allow navigation without saving any cookies or history

Only good to avoid parental/corporate control: today most web services track the IP number of the device

CONTAINERS

limit the ability of some site, eg Facebook, to track:

the *like* and *follow* buttons embedded elsewhere can create user tracking well beyond the visit to FB’s own page

FB might even track you visiting pages you don’t *like* nor *share*

It is unclear whether one can 100% avoid FB tracking

A recommended solution is multi-account containers

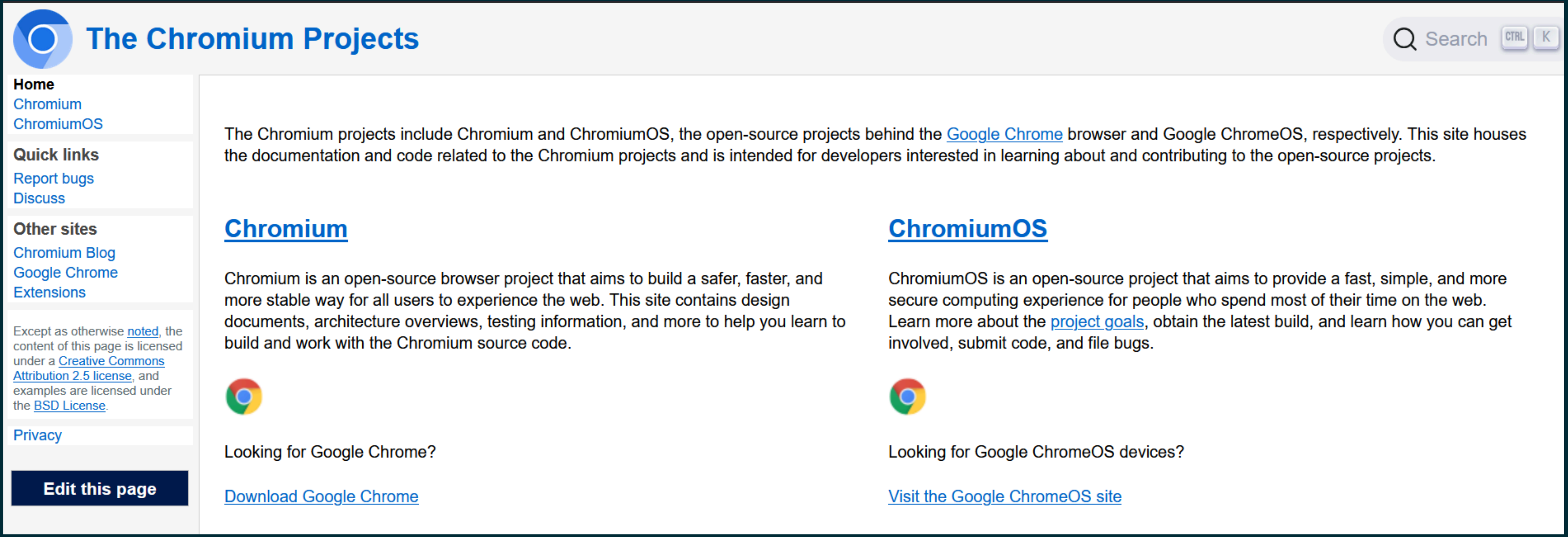
NON-CHROME BROWSER

Chrome is built around an excellent *page rendering software*

However, it basically tracks your navigation to see where you go when you **jump out** of site:

that is the only part of navigation that the server-side cannot see

Moreover, Chrome converts the action of *typing* a URL into *searching* a URL



Except as otherwise noted, the content of this page is licensed under a Creative Commons Attribution 2.5 license, and examples are licensed under the BSD License.

The Chromium projects include Chromium and ChromiumOS, the open-source projects behind the Google Chrome browser and Google ChromeOS, respectively. This site houses the documentation and code related to the Chromium projects and is intended for developers interested in learning about and contributing to the open-source projects.

Chromium

Chromium is an open-source browser project that aims to build a safer, faster, and more stable way for all users to experience the web. This site contains design documents, architecture overviews, testing information, and more to help you learn to build and work with the Chromium source code.

Looking for Google Chrome?

Download Google Chrome

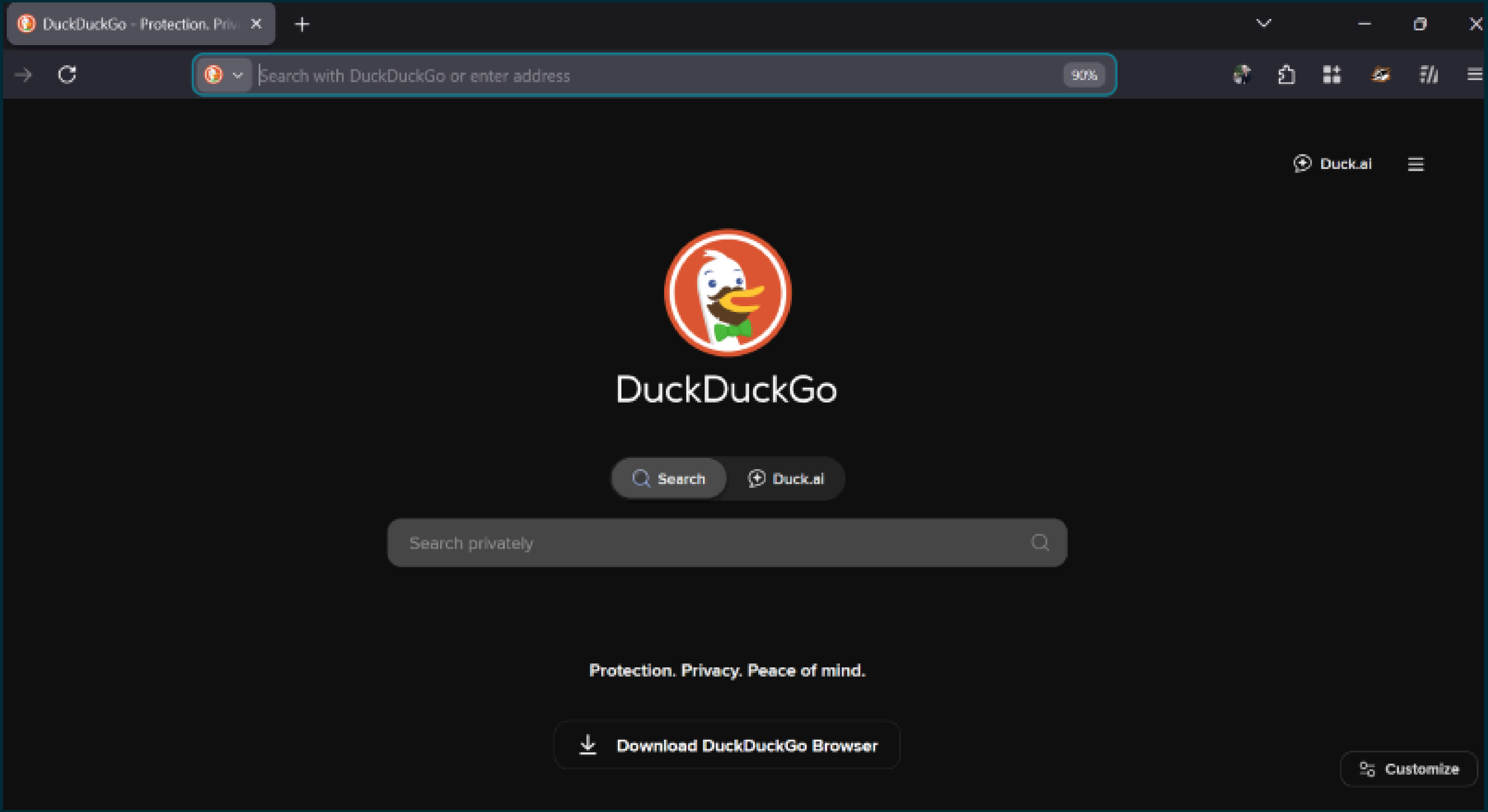
ChromiumOS

ChromiumOS is an open-source project that aims to provide a fast, simple, and more secure computing experience for people who spend most of their time on the web. Learn more about the project goals, obtain the latest build, and learn how you can get involved, submit code, and file bugs.

Looking for Google ChromeOS devices?

Visit the Google ChromeOS site

Google releases (at least for now) the Chromium version of Chrome, which is lighter and less tracking


DuckDuckGo - Protection. Priv
Search with DuckDuckGo or enter address
90%
Duck.ai
DuckDuckGo
Search
Duck.ai
Search privately
Protection. Privacy. Peace of mind.
Download DuckDuckGo Browser
Customize

Use DuckDuckGo

NON-GOOGLE SEARCH

Don’t log into Google services unless you have to (I have to)

Use the DuckDuckGo aggregator for your searches

DuckDuckGo collects search requests and passes them over to Google in batches

ACADEMIC RESEARCH

A MODEL OF WEB NAVIGATION

The Potential Gain model rates the most central, (i.e., influential) pages when accounting for the ‘jumps’ in human web navigation

We say that a network N is navigable when an agent is able to efficiently reach any target node in N by means of local routing decisions

In a social network, navigability translates into the ability of reaching an individual through personal contacts

POTENTIAL GAIN, CONT’D

Graph navigability is well-studied, but a fundamental question is still open:

why some people more likely than others to be reached via short, friend-of-a-friend, communication chains?

We propose a model of human navigation on networks that explains this phenomenon

Open access preprint

Couldn't load plugin.

PDF embedding failed… this browser does not support it.

EMBEDDING PDFS

```html
<object data="https://arxiv.org/pdf/2005.08959.pdf" type="application/pdf" width="
    <embed src="https://arxiv.org/pdf/2005.08959.pdf">
        <p>PDF embedding failed... this browser does not support it.</p>
    </embed>
</object>
```

THREE PRIVACY TOOLS

PRIVACY BADGER

A browser extension, the Privacy Badger disables tracking cookies, supercookies etc.

Probably the best overall solution now available

“If an advertiser seems to be tracking you across multiple websites without your permission, Privacy Badger automatically blocks that advertiser from loading any more content in your browser. To the advertiser, it’s like you suddenly disappeared.”

AD OBSERVER

A brower extension: get it for Firefox

An academic project developed by the NYU Cybersecurity fo Democracy project

Currently focussed on US politics ads on FB

It collects and make public what information and what advertisements are served up by FB, Google etc. and to which audience.

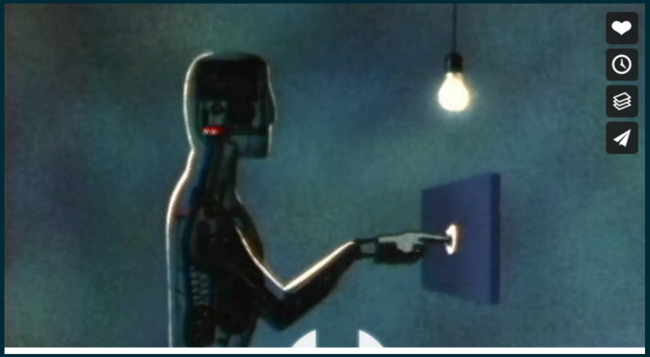
under heavy *legal fire* from Meta etc.: the ultimate endorsement in terms of creating web privacy.

AD NAUSEAM

Another browser add-on

it fights profiling in a *starkly different way*:

instead of denying access to the clicks and likes,



see video here

it **spoil** the signal coming from our web activity to the maximum entropy (minimum information content).