



ENIGMA

The Browser Privacy Arms Race

Which Browsers Actually Protect Your Privacy?

Andrés Arrieta - Dir of Consumer Privacy Engineering

Who are we?



Non-profit that fights for your civil liberties in the digital world.

- Certbot, HTTPS Everywhere, Panopticlick, Privacy Badger...
- AI, Coders Rights, Freedom of Speech, Privacy...

We fight for the users

Why does it matter?

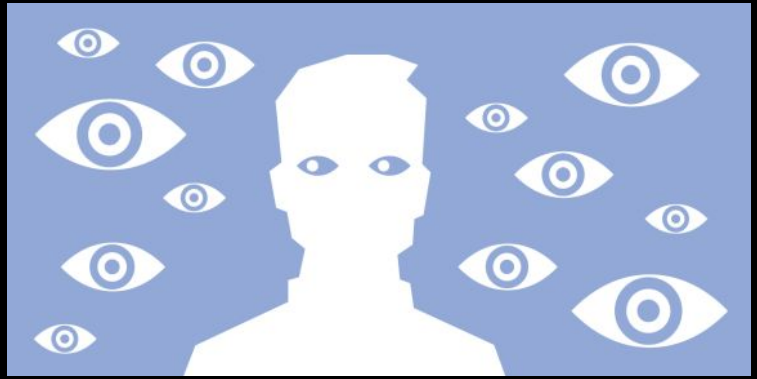
Browsers are most users' window the Internet, and most users do not change the defaults.

The out of the box window to the Internet defines the defaults for the rights most users enjoy.

The Internet should be opt-in and empower users where the default is respecting our rights

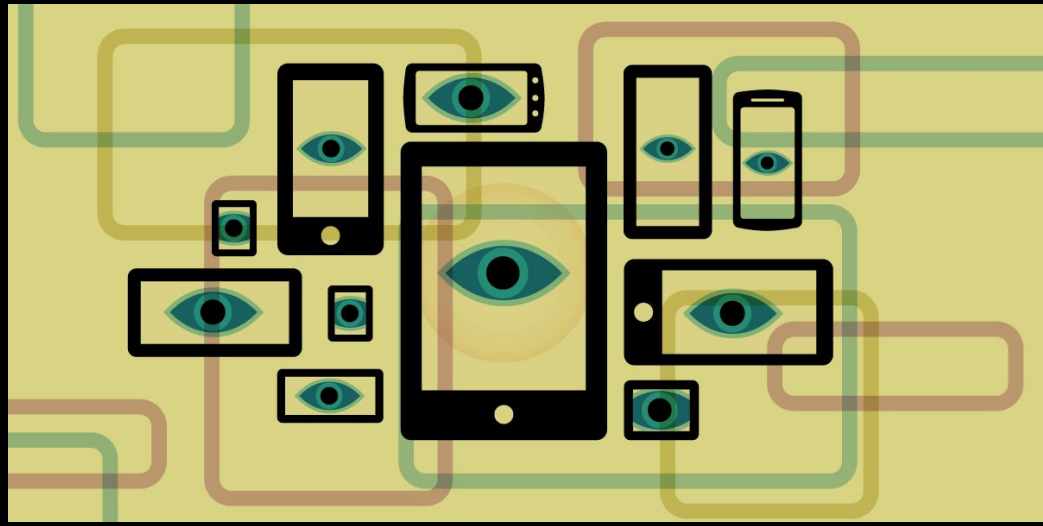
Who cares about more relevant ads anyway?

So what if they gather some information?



What can third-parties learn from your browser or other sources?

- Age
- Gender
- Race
- Address physical and email
- Location
- Browser
- Device
- Time spent
- What you clicked
- What you hovered
- What you buy online and offline
- Health data



They can learn directly or infer a lot of things from your browsing habits!

- Politics
- Health condition
- Religious beliefs
- Sexual orientation
- Hobbies and interests
- **Personality**
- Where you are going
- Who you know and who you've met





What can they do with it?

- Marketing for more “relevant” ads (That you probably learned to ignore)
- Decide what you see from your friends
- Decide what news and which outlets you see
- Decide what you should interact with (what has more engagement)

EFF

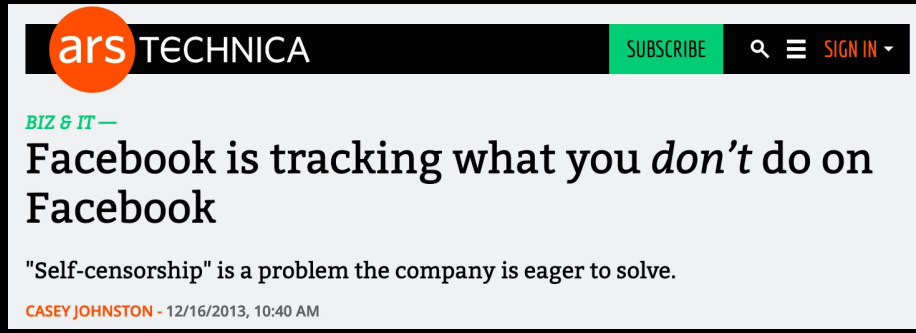
Trigger psychological buttons

- Anger
- Happiness
- Depresion
- Fear









What are the browsers doing?

Apple - Safari/Webkit



- \+ ITP
  - Battles with Criteo
- \+ Large anonymity sets
- \- No extensions

Brave



- + HTTPS Everywhere built-in
- + Anti-fingerprinting built-in
- + Easylist blocking
- + Chromium extensions

Mozilla - Firefox



- + Disconnect tracker blocking
- + Widgets/Containers
- + Install 3rd party extensions

Tor



- + HTTPS Everywhere
- + Large anonymity pool
- + Anti Fingerprinting

Chrome



- + Removing fingerprinting vectors
- - No tracker-blocking
- - Killing meaningful privacy extensions
- - Proposals to make it easier to track and standardize it

Edge-ium?



- + Past versions of IE supported DNT
- + Tracking Protections
- ? Current Edge-ium supports extensions BUT

How do their efforts stack up?

Actions and plans

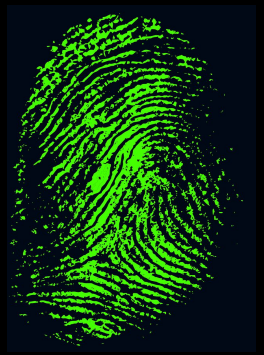
These are not grades!

✅ Doesn’t mean they’re all good and done

How do they stack up?

Fingerprinting

- **Firefox** - Blocks known 3rd parties
- **Chrome** - Reduce UA
- **Safari** - Canvas Fingerprinting
- **Tor** - Effort to make all =
- **Brave** - No access to commonly used
- **Edge** - Same as Chromium



How do they stack up?

Fingerprinting

- **Low hanging fruit**
- **Try to make as large as possible the anonymity pool**

How do they stack up?

Large Anonymity Pool

- ? **Firefox**
- ? **Chrome**
- ✓ **Safari** - Controls the hardware
- ✓ **Tor**
- ? **Brave**
- ? **Edge**



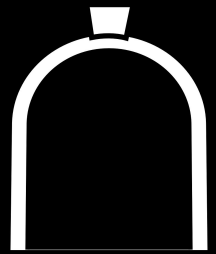
How do they stack up? Large Anonymity Pool

- How far can you remove features
- Consider hardware when comparing

How do they stack up?

eSNI/DoH/DoT/Tunneling

- **Firefox** - eSNI, DoH
- **Chrome** - DoH, eSNI?
- **Safari**
- **Tor** - Tor! And Firefox.
- **Brave** - DoH, eSNI?
- **Edge** - DoH



How do they stack up? eSNI/DoH/DoT/Tunneling

- **Third-parties on sites are not the only threat vector for privacy**
- **Allow users to choose**

How do they stack up?

Tracker Blocking

- **Firefox** - List, 3rd Party Cookies
- **Chrome**
- **Safari** - ITP
- **Tor** - Firefox's protections
- **Brave** - List, 3rd Party cookies
- **Edge** - List based



How do they stack up?

Tracker Blocking

- List vs Heuristics vs Behaviour
- Balance of protection vs breaking
- Transparency
- Control
- Choice

How do they stack up?

Extensions Real Privacy

- **Firefox**
- **Chrome** - Manifest V3
- **Safari** - Walled garden
- **Tor**
- **Brave**
- **Edge** - Follow Google or do better?



How do they stack up?

Extensions Real Privacy

- You serve the users, protect the users
- You can’t account for all threats, allow others to help
- Blunt solutions that do not provide real solutions aren’t solutions

EFF

					
Firefox	✓	?	✓	✓	✓
Chrome	✓	?	✓	✗	✗
Safari	✓	✓	✗	✓	✗
Tor	✓	✓	✓	✓	✓
Brave	✓	?	✓	✓	✓
Edge	✓	?	✓	✓	?

EFF

How do they stack up?

- Privacy is hard but there are easy lifts
- If privacy is too hard for you, maybe don’t get involved with making a browser?
- Ads != (always) tracking
- Money doesn’t make it ok to violate our rights

Some Challenges

- **Anonymity Pool:** Some have the advantage of controlling the hardware
- **Providing Privacy while having a good browsing experience**
  - More trackers blocked = faster and less noisy browsing
  - Too aggressive can brake functionality
  - User choice can help in many of these cases
- **Privacy vs Security**
  - They are different things but for some users they are the same
  - Investing in security doesn’t equate to investing in privacy
  - Users shouldn’t be forced to choose

What should you do?

- The Internet needs to be an **opt-in world**, not opt-out **(Users' choice)**
- The **default** has to be **security AND privacy**



Demand better, you shouldn't have to "choose" between privacy and security.

YOUR VOICE HAS MORE POWER THAN YOU THINK!



Thank you!

Andrés Arrieta - Director of Consumer Privacy Engineering
andres@eff.org