



Data Privacy Detective Podcast – Episode 64: The Two Faces of Browsers and Our Privacy Options

Apr 02, 2021

Categories:

[Blogs](#)

[Podcast](#)

[Technology Blog](#)

Authors:

[Joseph J. Dehner](#)

Janus was the Roman god of doors, gates, and transitions. He needed two faces to look in both directions – life and death, past and future. Internet browsers allow us to access and gaze across the internet, but at the same time, they are watching us, recording what we do while browsing. Our browsing data becomes a growing personal archive about us.

After accumulating “big data” about millions or billions of people, browser businesses monetize it by sharing the data with advertisers and others for a price paid to them. This business model does not require them to share the identity of each person using their browser, but neither does it require them to pay us for using and sharing our data. By amassing our browsing history, browsers and their affiliates hold vast amounts of private information. Browsers do not charge us – browsing is free. But as it is said, when a product is free, we become the product – or more specifically, our data becomes the product.

Google’s Chrome is the giant of the browsing sector, amounting to 63.59% of global browsing usage according to one source. [StatCounter Global Stats – Browser, OS, Search Engine including Mobile Usage Share](#) (Feb. 2021). Apple’s Safari holds second place, followed by a wide margin by browsers each holding less than a 4% share including Firefox, Edge, Samsung Internet, Opera, and Brave. These companies assure users that they do not share individual names or email addresses with third parties, at least not without user permission. Each offers differing privacy features within their settings.

Browsers can be ranked by their privacy orientation. Avast, for example, issued such January 2021 rankings – [Best Web Browsers for Privacy & Security in 2021 | Avast](#) . It rated Chrome as “not the best” for privacy and security. Chrome offers features for users to choose their privacy settings, such as Do Not Track (found under

Show Advanced Settings). Some choices available through Chrome settings allow a user, for example, to stop visited websites from sharing targeted ads, but do not stop websites from collecting visitor data. Google offers a guide to set your privacy settings at [Choose your privacy settings – Computer – Google Chrome Help](#).

Avast found Safari more secure than Chrome by including such features as blocking by default third-party cookies and preventing cross-site tracking, though it commented that Safari includes no adblocking software without a user's adding a third-party browser extension to address that. Safari offers a password management feature. Safari uses Chrome's Safe Browsing lists to combat malicious sites, but Safari sends data to Google.

Avast rated other browsers as more privacy-oriented than Chrome or Safari. Firefox, through its non-profit "Manifesto" – [The Mozilla Manifesto](#) – has privacy-related features such as blocking of browser fingerprinting. Avast reports, however, that Firefox sends its browser data to Mozilla headquarters unless a user opts out of granting such permission. Avast considers Opera safe but mentions that Opera "helps itself" to users' data. Edge, successor to Internet Explorer and the default browser on Windows devices, is reported to send information about both device and data to its owner Microsoft, though Edge no longer sends personal identifiers to Microsoft servers according to an October 2020 report– [Google's Chrome versus everyone else: The best web browsers for privacy – Vox](#). Avast itself has a browser called Avast Secure Browser, which it promotes as having a built-in privacy and security suite, with ad blocking, anti-phishing, anti-tracking, and automatic HTTPS encryption. [Avast Secure Browser | Private browser from Avast](#).

Then there's TOR, which "prioritizes privacy above all else," according to Avast. TOR's call is this – "Defend yourself against tracking and surveillance." Traffic is encrypted and routed through nodes so that an ISP does not know what a user is accessing. It does not store browsing history. It deletes cookies and disrupts browser fingerprinting (a method to identify users when the email address is not directly known). TOR's VPN hides a person's IP address and encrypts the connection so that personal information about the user is hidden from advertisers and others while browsing. But ISPs

of those using TOR know that a person is using TOR, and it's not considered as usable or convenient as other browsers. By its nature, TOR is used by persons who wish to escape scrutiny from law enforcement and may intend to browse for less than legitimate purposes. Many companies prevent employees from using TOR while on company equipment.

This podcast episode is a conversation with the founder and CEO of Cocoon, an alternative browser. Unlike privacy add-ons like Privacy Badger, DuckDuckGo, or Ghostery, Cocoon is a browser. It was founded for the purpose of providing a more privacy-secure experience than any other browser. It provides a secure encrypted connection to the internet, anonymizing the user. It is built upon an open-source platform. Cocoon creates its name – a cocoon – around the browsing individual. It records and keeps data only in Cocoon's private cloud.

Its approach to monetization relies on anonymized data sharing, with a twist. Cocoon offers users the opportunity to share revenue collected from third parties. Its slogan is "It's your data – You should be the one to profit from it." Browsing on Cocoon can return a monthly amount to a truck driver of \$15-30 a month, for example, even as the truck driver is not personally identified in data that is shared to generate the revenue to be shared between Cocoon and users.

This podcast explores how browsers and privacy intersect, how users have choices – which browser to use, how to adjust privacy settings offered by browsers, and what add-ons to consider for browsing. What level of privacy to choose is within the control of a user.

If you have ideas for more interviews or stories, please email info@thedataprivacydetective.com.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.