L'Audit Invisible : Enquête Approfondie sur les Infrastructures de Surveillance et les Modèles Économiques des Navigateurs Web Modernes

L'évolution du navigateur web, passant d'un simple moteur de rendu de documents à un environnement d'exécution d'applications complexes, a transformé cet outil en le capteur le plus granulaire de l'identité numérique contemporaine. Dans cet écosystème, la gratuité apparente des logiciels masque une infrastructure de capture de données dont la sophistication rivalise avec les systèmes de renseignement étatiques. Cette enquête déconstruit les mécanismes techniques par lesquels les six principaux navigateurs du marché — Google Chrome, Microsoft Edge, Mozilla Firefox, Brave, Opera et Apple Safari — traitent l'activité humaine comme une matière première. En analysant les flux de données sortants, les identifiants uniques et les modèles de monétisation, l'analyse révèle que le choix d'un navigateur n'est pas seulement une question d'ergonomie, mais un acte de positionnement dans l'économie de la surveillance globale.

La Télémétrie contre l'Espionnage : Une Frontière Technique de Sable

La distinction entre la télémétrie légitime et l'espionnage comportemental est le premier champ de bataille de la confidentialité des données. Théoriquement, la télémétrie se limite à la collecte de données de diagnostic nécessaires à l'amélioration de la stabilité et des performances du logiciel, telles que les rapports de plantage, l'utilisation des ressources système ou la latence du réseau.[1] Cependant, l'intégration d'identifiants uniques (UID) transforme ces statistiques opérationnelles en traces comportementales persistantes, permettant aux éditeurs de reconstruire des historiques de navigation détaillés, souvent à l'insu de l'utilisateur.[3]

La Mécanique des Identifiants Uniques

Le risque pour la vie privée réside moins dans la donnée brute que dans la persistance et l'entropie de l'identifiant qui lui est rattaché. Un identifiant qui survit au redémarrage de l'application ou, plus grave, à une réinstallation du système, permet de lier des sessions de navigation disjointes dans le temps et l'espace. Les études académiques menées par le professeur Douglas Leith démontrent que les navigateurs se divisent en catégories distinctes selon la nature des identifiants qu'ils transmettent à leurs serveurs centraux.[2]

Navigateur	Nature de l'Identifiant (UID)	Persistance Technique	Risque de Profilage
Brave	Identifiants éphémères	Réinitialisation à chaque session	Faible ; empêche la corrélation temporelle.[5]
Google Chrome	ID d'instance (X-Client-Data)	Persiste jusqu'à la réinstallation	Modéré à Élevé ; lié au compte Google.[1]
Mozilla Firefox	Client ID / Telemetry ID	Persiste par défaut (supprimable)	Modéré ; lié à l'instance logicielle.[8]
Apple Safari	Identifiants iCloud / Device ID	Lié au matériel et au compte	Élevé ; corrélation multi-appareils.[1]
Microsoft Edge	Hardware UUID (ID matériel)	Immuable (lié à la machine)	Critique ; survit au formatage.[3]
Opera	Ad-ID / Installation ID	Persiste avec le profil utilisateur	Élevé ; partagé avec des tiers.[10]

L'audit technique révèle que Microsoft Edge et Yandex occupent l'extrémité la plus intrusive du spectre. Contrairement à Chrome ou Firefox, qui lient principalement les données à une installation logicielle, Edge transmet le UUID (Universally Unique Identifier) du matériel. Cette pratique permet à Microsoft de suivre non seulement le navigateur, mais l'appareil physique lui-même, créant un lien indélébile entre l'activité numérique et le silicium de l'hôte.[4] Même si Microsoft affirme que ces données servent à l'amélioration du produit, la présence d'un identifiant matériel immuable rend toute promesse d'anonymisation techniquement caduque, car les données peuvent être corrélées avec d'autres services de l'écosystème Windows.[13]

Le Flux de Données "Safe Browsing" et ses Dérives

Tous les navigateurs majeurs intègrent un service de protection contre les sites malveillants, généralement basé sur l'API Google Safe Browsing.[6] Le mécanisme standard repose sur le téléchargement de listes de hachages de sites dangereux. Toutefois, l'activation des options de "protection renforcée" modifie ce comportement : le navigateur envoie en temps réel les URLs complètes ou des hachages partiels aux serveurs de l'éditeur pour vérification. Ce qui est présenté comme une fonctionnalité de sécurité devient alors un flux d'espionnage comportemental légitimé, offrant à l'éditeur une vue exhaustive de la navigation, y compris sur

des réseaux privés ou des pages sensibles.[16]

Modèles Économiques : Jardins Clos contre Marchands de Données

La déconstruction du modèle économique des navigateurs est essentielle pour comprendre la destination finale des flux de données. La monétisation suit deux logiques divergentes : le maintien d'un monopole publicitaire interne (Walled Garden) et l'exploitation de partenariats avec des courtiers de données (Data Brokers).

Le Modèle du "Walled Garden" (Google, Apple, Microsoft)

Pour les géants de la technologie, la donnée brute est une ressource trop précieuse pour être vendue. Leur stratégie consiste à enfermer l'utilisateur dans un écosystème où ils sont les seuls à pouvoir traiter et valoriser l'information. Dans ce modèle, le navigateur est un outil de captation qui alimente une régie publicitaire interne.[18]

Google Chrome n'a pas besoin de vendre les données de navigation car il les utilise pour affiner les profils publicitaires au sein de Google Ads. L'annonceur n'achète pas la liste des sites visités par un individu, mais l'accès à une audience segmentée par le navigateur.[20] Cette approche, bien que protégeant la donnée contre les tiers "extérieurs", renforce un pouvoir de surveillance centralisé où l'éditeur possède une connaissance omnisciente de l'utilisateur, de ses recherches (Search) à ses communications (Gmail) et sa navigation (Chrome).[19] Apple, malgré une rhétorique axée sur la vie privée, suit une logique identique avec Safari, limitant le tracking par les tiers pour favoriser son propre réseau publicitaire et renforcer l'adhérence à son matériel.[23]

Le Modèle d'Exploitation Ouverte (Opera, Partenariats Tiers)

À l'inverse des jardins clos, des navigateurs comme Opera adoptent un modèle plus fragmenté, dépendant de partenariats directs avec des régies publicitaires et des services tiers. Depuis son acquisition par le consortium chinois Kunlun Tech, Opera a transformé son navigateur en une plateforme de services intégrés, incluant des flux de nouvelles, des outils de cashback et des services de fintech.[10]

L'analyse de la politique de confidentialité d'Opera révèle une structure complexe où les données sont partagées avec des partenaires comme Takeads pour la monétisation contextuelle et l'affiliation.[11] Ici, le navigateur agit comme un agent commercial, injectant des signets prédéfinis (Speed Dial) et des publicités natives directement dans l'interface utilisateur. La monétisation repose sur la vente d'accès et de signaux comportementaux à un réseau étendu de tiers, ce qui multiplie les points de fuite potentiels pour les données personnelles.[10]

Le Scandale du Real-Time Bidding (RTB) : Le Navigateur comme Complice

Le Real-Time Bidding (RTB) représente l'apogée de l'extraction de données automatisée. Chaque fois qu'une page web contenant des publicités se charge, une enchère se produit en quelques millisecondes pour déterminer quelle publicité sera affichée. Ce processus déclenche l'envoi d'une "bid request" (demande d'enchère) qui contient des informations intimes sur l'utilisateur.[29]

La Mécanique de la Fuite de Données

Lorsqu'un utilisateur visite un site web, le navigateur exécute des scripts publicitaires qui collectent et transmettent des données à des Ad Exchanges. Ces données incluent souvent la localisation précise, les identifiants de cookies, le type d'appareil, mais aussi le titre et l'URL de la page consultée. Le scandale réside dans la diffusion massive : une bid request est envoyée à des centaines d'entreprises de publicité simultanément.[31]

Donnée fuitée via RTB	Implication pour la Vie Privée
URL de la page	Révèle les intérêts politiques, médicaux ou sexuels.[33]
Localisation (IP/GPS)	Permet de suivre les déplacements physiques.[29]
Cookie ID / IFA	Lie la session actuelle à des dossiers historiques.[30]
User-Agent String	Facilite le fingerprinting unique de l'appareil.[34]

Les navigateurs facilitent cette fuite en autorisant par défaut les cookies tiers (cas de Chrome jusqu'en 2025) ou en ne bloquant pas les scripts de tracking invasifs. Bien que Google propose de remplacer les cookies tiers par son API "Topics", les critiques soulignent que cela ne fait que déplacer le contrôle de la fuite vers Google, sans supprimer le profilage.[20] À l'inverse, des navigateurs comme Brave ou Firefox (en mode Strict) bloquent les communications avec les domaines connus de RTB, asséchant ainsi le flux de données vers l'écosystème des courtiers.[6]

Enquête sur les Géants : Profils Techniques Détaillés

Google Chrome : Le Double Jeu du "Privacy Sandbox"

Chrome occupe une position paradoxale. Techniquement, il offre l'une des architectures de sécurité les plus robustes, avec une isolation de site (sandboxing) de pointe qui protège contre les exploits de mémoire.[16] Cependant, cette sécurité sert de coffre-fort pour un système de collecte interne sans précédent. La télémétrie de Chrome est intrinsèquement liée aux services Google. Même lorsque la synchronisation est désactivée, le navigateur effectue des requêtes vers clients2.google.com contenant des jetons d'authentification et des identifiants de session.[7]

Le projet "Privacy Sandbox" est la réponse de Google aux critiques sur le tracking. Sous prétexte de supprimer les cookies tiers, Google introduit des APIs (Topics, Protected Audience) qui effectuent le profilage directement dans le navigateur.[21] L'analyse démontre que l'API Topics, qui classe les utilisateurs par centres d'intérêt, peut encore être utilisée pour le fingerprinting de groupes d'utilisateurs, maintenant ainsi la capacité de ciblage tout en verrouillant le marché au profit de Google.[20]

Microsoft Edge : La Surveillance au Cœur de l'OS

Microsoft Edge a été identifié par plusieurs études indépendantes comme le navigateur le plus agressif en matière de collecte de données.[1] Son lien avec le système d'exploitation Windows lui permet de collecter des informations inaccessibles aux autres navigateurs. Par exemple, Edge transmet non seulement les URLs visitées pour le service de suggestion de recherche de Bing, mais il envoie également des données de navigation complètes à vortext.data.microsoft.com associées au Hardware UUID.[1]

Une controverse récente a mis en lumière que Edge modifiait certains cookies pour y insérer des codes d'affiliation Microsoft lors de visites sur des sites marchands, une pratique s'apparentant à du détournement de trafic.[37] De plus, l'intégration omniprésente de l'IA Copilot crée un flux constant de données sémantiques : le contenu des pages consultées est analysé en temps réel par les serveurs de Microsoft pour fournir des résumés ou des suggestions, annihilant toute notion de navigation locale.[14]

Mozilla Firefox : L'Indépendance Fragile

Firefox reste le seul navigateur majeur utilisant son propre moteur de rendu (Gecko), offrant une alternative réelle à l'hégémonie de Chromium. Cependant, par défaut, Firefox intègre une télémétrie "moyennement bavarde" qui collecte des données sur l'utilisation des fonctionnalités et des métadonnées de session via Glean.[8] Son modèle de revenus, largement dépendant de la redevance payée par Google pour être le moteur de recherche par défaut, crée une tension éthique évidente.[1]

Néanmoins, Firefox offre les outils de durcissement les plus avancés. Grâce à son interface about:config, un expert peut désactiver des fonctionnalités intrusives comme Pocket,

WebRTC (pour éviter les fuites d'IP) ou les services de localisation de Google.[40] L'initiative "Tor Uplift" a également permis d'intégrer des technologies de résistance au fingerprinting directement dans le cœur du navigateur, faisant de Firefox une base solide pour une navigation hautement sécurisée une fois configurée correctement.[40]

Brave : La Confidentialité comme Produit

Brave se distingue par une approche "Privacy-by-Default". Lors des tests réseau, c'est le navigateur qui effectue le moins de connexions vers ses serveurs d'origine.[6] Il utilise des identifiants qui sont réinitialisés à chaque redémarrage, empêchant ainsi la construction d'un profil à long terme.[5] Sa fonction native de blocage de publicités et de trackers est intégrée au moteur, ce qui la rend plus performante et plus difficile à contourner que les extensions traditionnelles.

Toutefois, le modèle de Brave repose sur une "économie de l'attention" alternative. Le système Brave Rewards encourage les utilisateurs à visionner des publicités sélectionnées par Brave en échange de jetons BAT.[42] Bien que ce système soit anonymisé et basé sur le traitement local, il maintient l'utilisateur dans une logique publicitaire. Par ailleurs, des erreurs passées, comme le partage de requêtes DNS dans les fenêtres Tor ou l'ajout automatique de liens d'affiliation, obligent à une vigilance continue sur les mises à jour du logiciel.[42]

Apple Safari : Le Rempart du Matériel

Safari est le précurseur de nombreuses technologies de confidentialité, notamment l'Intelligent Tracking Prevention (ITP) qui bloque les cookies tiers et fragmente le stockage local pour empêcher le suivi intersites.[23] Son architecture est conçue pour optimiser l'autonomie et la sécurité sur le matériel Apple. Il réduit également l'entropie du navigateur pour limiter le fingerprinting, en ne rapportant que des configurations système standard aux sites web.[23]

Le point faible de Safari réside dans son opacité. En tant que logiciel propriétaire, ses mécanismes internes ne sont pas auditables par la communauté. La synchronisation iCloud de l'historique et des mots de passe signifie que ces données résident sur les serveurs d'Apple. Bien que chiffrées, elles restent liées à l'identifiant Apple unique de l'utilisateur, facilitant une corrélation transversale entre l'activité web, l'utilisation des applications et la localisation physique via l'iPhone.[1]

Opera : L'Incertitude Juridictionnelle

Opera est devenu un "navigateur-service" dont le cœur de métier est la monétisation de l'audience. Sous contrôle de Kunlun Tech, l'entreprise doit théoriquement se conformer au RGPD car elle est basée en Norvège.[45] Cependant, la structure de propriété soulève des questions sur l'application de lois sur les données étrangères (comme la PIPL chinoise). Opera affirme que les données sont stockées sur des serveurs européens et qu'aucune autorité n'a

jamais accédé à ses journaux VPN.[45]

Techniquement, le navigateur est l'un des plus lourds en termes de requêtes publicitaires et de trackers tiers intégrés dès l'installation. Son "VPN" est en réalité un proxy de navigateur qui ne chiffre que le trafic HTTP d'Opera, laissant le reste du système exposé.[43] Pour un analyste, Opera représente un compromis risqué où les fonctionnalités de confort (limiteurs de RAM pour les joueurs, IA intégrée) sont payées par une exposition constante à des régies publicitaires et des collecteurs de données tiers.[10]

Durcissement de la Sécurité (Hardening) : Directives Techniques

Pour transformer un navigateur de capture en un outil de navigation sécurisé, une intervention sur les paramètres profonds est nécessaire.

Stratégies pour les Systèmes d'Entreprise (Edge/Chrome)

Dans un environnement géré, le durcissement passe par les modèles d'administration (GPO). Il est possible de désactiver les flux de données les plus critiques tout en maintenant la compatibilité.

Paramètre GPO / Registre	Valeur	Impact sur la Confidentialité
MetricsReportingEnabled	0 (False)	Désactive l'envoi de télémétrie et rapports de plantage.[49]
SearchSuggestEnabled	0 (False)	Empêche l'envoi de chaque caractère tapé aux serveurs de recherche.[50]
DiagnosticData (Edge)	0 (Off)	Coupe le lien entre le navigateur et le UUID matériel.[51]
SafeBrowsingProtectionLevel	1 (Standard)	Évite l'envoi des URLs complètes requis par le mode "Enhanced".[17]

PasswordManagerEnabled	0 (False)	Recommandé : utiliser un gestionnaire de mots de passe externe.

Configuration Avancée de Firefox

Pour les utilisateurs individuels, Firefox offre le meilleur levier de contrôle via about:config. Les modifications suivantes sont essentielles pour un profil "High Privacy" :

1. **Resist Fingerprinting** : Passer privacy.resistFingerprinting à true pour masquer les caractéristiques de l'appareil (polices, résolution, fuseau horaire).[40]
2. **Désactivation WebRTC** : Passer media.peerconnection.enabled à false pour empêcher la découverte de l'adresse IP locale derrière un VPN.[40]
3. **Partitionnement des Cookies** : S'assurer que network.cookie.cookieBehavior est réglé sur 4 ou 5 pour isoler les cookies par site.
4. **Désactivation des Pings** : Passer browser.send_pings à false pour bloquer le suivi des clics par les sites web.[40]

Le Cas Particulier du CNAME Cloaking

Une technique moderne de tracking consiste à utiliser des alias DNS (CNAME) pour faire passer un tracker tiers pour un sous-domaine de confiance du site visité. La plupart des bloqueurs de pubs classiques échouent face à cela. Firefox et Brave sont actuellement les seuls navigateurs offrant des capacités techniques pour démasquer ces requêtes et bloquer les fuites de données invisibles.[52]

Analyse des Risques et Verdict de l'Analyste

La confrontation des données collectées permet d'établir un verdict clair sur la posture de confidentialité de chaque solution. La notion de "sécurité" doit ici être scindée : la sécurité contre les attaquants externes (où Chrome et Edge excellent grâce à leurs ressources d'ingénierie) et la sécurité contre l'éditeur lui-même (où ils échouent).

Classement par "Bavardage" (Du plus silencieux au plus indiscret)

1. **Brave** : Le plus silencieux. Pas d'identifiants persistants par défaut, blocage agressif des trackers et du RTB.[5]
2. **Firefox (Hardened)** : Équivalent à Brave s'il est configuré correctement. Permet une isolation totale mais demande une expertise technique.[39]
3. **Safari** : Bon élève pour le grand public, mais verrouillé dans l'écosystème Apple. Très efficace contre le tracking publicitaire de masse.[23]
4. **Firefox (Default)** : Correct, mais souffre de sa dépendance à Google et de sa télémétrie native.[8]
5. **Google Chrome** : Le pilier de la surveillance publicitaire. Sécurisé techniquement, mais

indiscret par construction économique.[1]

6. **Opera** : Profilage publicitaire intégré et flou juridictionnel. Un choix axé sur les fonctionnalités, pas sur la vie privée.[10]
7. **Microsoft Edge** : Le plus intrusif. La collecte d'identifiants matériels immuables et le lien avec l'OS en font une menace persistante pour l'anonymat.[1]

Conclusion : Le Navigateur, Terminal de l'Économie de l'Attention

L'enquête démontre que le navigateur web est devenu l'instrument de mesure principal de l'économie de la surveillance. Alors que les techniques de tracking traditionnelles (cookies) sont en déclin, les éditeurs migrent vers des méthodes plus profondes : fingerprinting, identifiants matériels et analyse sémantique par IA.

Pour l'expert en cyber-sécurité, le constat est sans appel : la gratuité est un leurre qui finance une infrastructure d'extraction de valeur comportementale. Le passage de Chrome au Privacy Sandbox ne marque pas la fin du tracking, mais sa nationalisation par Google. La persistance de Microsoft Edge à collecter des UUID matériels souligne une volonté de lier l'identité numérique à l'identité physique de manière irréversible.

La recommandation finale pour toute entité ou individu soucieux de sa souveraineté numérique est d'adopter une stratégie de défense en profondeur. Cela implique non seulement le choix d'un navigateur silencieux (Brave ou Firefox configuré), mais aussi l'utilisation systématique de couches d'anonymisation (VPN, DNS sécurisé) et une vigilance constante sur les nouvelles fonctionnalités "assistées par l'IA" qui ne sont, en réalité, que de nouvelles fenêtres ouvertes sur l'intimité numérique. Le navigateur ne doit plus être considéré comme une fenêtre sur le monde, mais comme une interface filtrée qui doit être durcie pour protéger l'utilisateur du monde qui l'observe.

Ouvrages cités

1. Telemetry - Dr. Mike Murphy, dernier accès : février 11, 2026, https://ww2.coastal.edu/mmurphy2/oer/privacy/internet/telemetry/
2. Web Browser Privacy: What Do Browsers Say When They Phone ..., dernier accès : février 11, 2026, https://www.scss.tcd.ie/Doug.Leith/pubs/browser_privacy.pdf
3. If you're serious about browser privacy, you should probably pass on Edge or Yandex, claims Dublin professor - The Register, dernier accès : février 11, 2026, https://www.theregister.com/2020/02/27/edge_and_yandex_browser_privacy_shame/
4. Microsoft Edge branded as 'worrisome' for user privacy | IT Pro - ITPro, dernier accès : février 11, 2026, https://www.itpro.com/security/privacy/355029/microsoft-edge-branded-as-worrisome-for-user-privacy

5. Brave beats other browsers in privacy study | SOPHOS, dernier accès : février 11, 2026, https://www.sophos.com/fr-fr/blog/brave-beats-other-browsers-in-privacy-study
6. (PDF) Web Browser Privacy: What Do Browsers Say When They Phone Home?, dernier accès : février 11, 2026, https://www.researchgate.net/publication/349979628_Web_Browser_Privacy_What_Do_Browsers_Say_When_They_Phone_Home
7. What Do Browsers Say When They Phone Home?, dernier accès : février 11, 2026, https://www.scss.tcd.ie/Doug.Leith/pubs/additional_material.pdf
8. Which is the best browser for privacy in 2026? - Proton, dernier accès : février 11, 2026, https://proton.me/blog/best-browser-for-privacy
9. Web Browser Privacy: What Do Browsers Say When They Phone Home? - EndeavourOS Forum, dernier accès : février 11, 2026, https://forum.endeavouros.com/t/web-browser-privacy-what-do-browsers-say-when-they-phone-home/73953
10. What is Opera's business model? - Vizologi, dernier accès : février 11, 2026, https://vizologi.com/business-strategy-canvas/opera-business-model-canvas/
11. Privacy Policy - Opera Group Limited, dernier accès : février 11, 2026, https://www.operalimited.com/privacy-policy
12. Microsoft Edge browser flunks privacy test, Redmond cries foul - Windows Central, dernier accès : février 11, 2026, https://www.windowscentral.com/microsoft-edge-browser-flunks-privacy-test
13. A professor says Edge is the worst for privacy. Microsoft isn't happy - ZDNET, dernier accès : février 11, 2026, https://www.zdnet.com/article/a-professor-says-edge-is-the-worst-for-privacy-microsoft-isnt-happy/
14. User data and privacy in Microsoft Edge, dernier accès : février 11, 2026, https://learn.microsoft.com/en-us/legal/microsoft-edge/privacy
15. Privacy and Security Comparison of Web Browsers: A Review - ResearchGate, dernier accès : février 11, 2026, https://www.researchgate.net/publication/359624123_Privacy_and_Security_Comparison_of_Web_Browsers_A_Review
16. Safest Browsers 2025: Chrome vs Brave vs Firefox Security - Deepak Gupta, dernier accès : février 11, 2026, https://guptadeepak.com/browser-security-landscape-transformed-in-2025/
17. Your Solution for Secure Enterprise Browsing, dernier accès : février 11, 2026, https://chromeenterprise.google/solutions/secure-browsing/
18. Beyond Walled Gardens: How Marketers Can Thrive in a Fragmented Digital Landscape, dernier accès : février 11, 2026, https://www.northbeam.io/blog/walled-gardens-digital-marketing-advertising
19. The Data-Driven Economy (Chapter 2) - Regulating Access and Transfer of Data, dernier accès : février 11, 2026, https://www.cambridge.org/core/books/regulating-access-and-transfer-of-data/datadriven-economy/1CE21A2CCE5EB1ECA4B3F1769B02BC37

20. A Public and Reproducible Assessment of the Topics API on Real Data - arXiv, dernier accès : février 11, 2026, https://arxiv.org/html/2403.19577v2
21. Understanding Google's Privacy Sandbox and Its Impact on Advertising - Avenga, dernier accès : février 11, 2026, https://www.avenga.com/magazine/chrome-privacy-sandbox-explained/
22. Valuing Social Data - Colorado Law Scholarly Commons, dernier accès : février 11, 2026, https://scholar.law.colorado.edu/context/faculty-articles/article/2645/viewcontent/2024_Parsons_Valuing_Social_Data.pdf
23. Is Safari safe for privacy? What you need to know - Express VPN, dernier accès : février 11, 2026, https://www.expressvpn.com/blog/is-safari-safe/
24. The Best Web Browser in 2025 | Magic Lasso Adblock, dernier accès : février 11, 2026, https://www.magiclasso.co/insights/best-web-browser-2025/
25. Opera Limited (OPRA): history, ownership, mission, how it works & makes money, dernier accès : février 11, 2026, https://www.dcfmodeling.com/blogs/history/opra-history-mission-ownership
26. 2.3x revenue growth in a year — Opera's success story with Takeads - Blog, dernier accès : février 11, 2026, https://takeads.com/blog/opera-success-story/
27. Opera: Niche browser with 43.3% upside potential and 4.8% dividend yield - Freedom24, dernier accès : février 11, 2026, https://freedom24.com/ideas/details/18812
28. Opera Ads | Audience Solutions, dernier accès : février 11, 2026, https://www.opera.com/programmatic
29. Unpacking Real Time Bidding through FTC's case on Mobilewalla, dernier accès : février 11, 2026, https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/12/unpacking-real-time-bidding-through-ftcs-case-mobilewalla
30. THE COOKIE CHRONICLES. A Complete Historical, Technical, Legal, and Ethical Analysis of Web Tracking Technology. How Small Files Became the Foundation of Surveillance Capitalism. | by Global Audiences | Medium, dernier accès : février 11, 2026, https://medium.com/@global.audiences/the-cookie-chronicles-9a5b3096f7a7
31. DAD0085 - Evidence on Democracy and Digital Technologies - UK Parliament Committees, dernier accès : février 11, 2026, https://committees.parliament.uk/writtenevidence/106176/html/
32. A summary of the ICO report on RTB - and what happens next - Brave, dernier accès : février 11, 2026, https://brave.com/blog/ico-adtech-update-rtb/
33. RTB evidence - Brave, dernier accès : février 11, 2026, https://brave.com/rtb-evidence/
34. Beyond Cookies: The Sneaky Ways Websites Identify and Track You Online | TWiT.TV, dernier accès : février 11, 2026, https://twit.tv/posts/tech/beyond-cookies-sneaky-ways-websites-identify-and-track-you-online
35. Get to know the new Topics API for Privacy Sandbox - Google Blog, dernier accès : février 11, 2026,

https://blog.google/products-and-platforms/products/chrome/get-know-new-topics-api-privacy-sandbox/
36. Privacy Sandbox Progress Report - GOV.UK, dernier accès : février 11, 2026, https://assets.publishing.service.gov.uk/media/679cbbca3bd16ee4b57adf25/google_q4_2024_report.pdf
37. Like Honey, Microsoft Edge also altered cookies to steal affiliate link - YouTube - Reddit, dernier accès : février 11, 2026, https://www.reddit.com/r/MicrosoftEdge/comments/1pst4bb/like_honey_microsoft_edge_also_altered_cookies_to/
38. Chrome, Edge, Firefox, Opera, or Safari? We Pick the Best Browser for 2026 | PCMag, dernier accès : février 11, 2026, https://www.pcmag.com/picks/chrome-edge-firefox-opera-or-safari-we-pick-the-best-browser
39. Remove Non-Hardened Firefox / Firefox Without Arkenfox - Privacy Guides Community, dernier accès : février 11, 2026, https://discuss.privacyguides.net/t/remove-non-hardened-firefox-firefox-without-arkenfox/29260
40. How to Set Up Firefox for Privacy | Avoid the Hack (avoidthehack!), dernier accès : février 11, 2026, https://avoidthehack.com/firefox-privacy-config
41. Add Betterfox - Tool Suggestions - Privacy Guides Community, dernier accès : février 11, 2026, https://discuss.privacyguides.net/t/add-betterfox/32517
42. Brave (web browser) - Wikipedia, dernier accès : février 11, 2026, https://en.wikipedia.org/wiki/Brave_(web_browser)
43. The best browsers for privacy in 2026 - Surfshark, dernier accès : février 11, 2026, https://surfshark.com/blog/what-is-the-best-browser-for-privacy
44. Keep your browsing history private in Safari and Maps - Apple Support, dernier accès : février 11, 2026, https://support.apple.com/guide/personal-safety/keep-your-browsing-history-private-ips375e6d608/web
45. General reliability, security and privacy of Opera, dernier accès : février 11, 2026, https://forums.opera.com/topic/84462/general-reliability-security-and-privacy-of-opera
46. Is Opera's userbase still protected by the GDPR if Opera is now majority-owned by a Chinese company? : r/OperaGX - Reddit, dernier accès : février 11, 2026, https://www.reddit.com/r/OperaGX/comments/1ok4hmq/is_operas_userbase_still_protected_by_the_gdpr_if/
47. Transparency Report - Opera Security Team, dernier accès : février 11, 2026, https://security.opera.com/en/opera-transparency-report/
48. Is Opera GX Spyware? Here's What You Need to Know - Comparitech, dernier accès : février 11, 2026, https://www.comparitech.com/blog/information-security/is-opera-gx-spyware/
49. Microsoft Edge Browser Policy Documentation MetricsReportingEnabled, dernier accès : février 11, 2026, https://learn.microsoft.com/en-us/deployedge/microsoft-edge-browser-policies/metricsreportingenabled

50. Security and privacy policies - Chrome Enterprise and Education Help, dernier accès : février 11, 2026, https://support.google.com/chrome/a/answer/9036555?hl=en
51. Microsoft Edge enterprise privacy settings, dernier accès : février 11, 2026, https://learn.microsoft.com/en-us/deployedge/microsoft-edge-enterprise-privacy-settings
52. Large-scale Analysis of DNS-based Tracking Evasion - broad data leaks included?, dernier accès : février 11, 2026, https://blog.lukaszolejnik.com/large-scale-analysis-of-dns-based-tracking-evasion-broad-data-leaks-included/