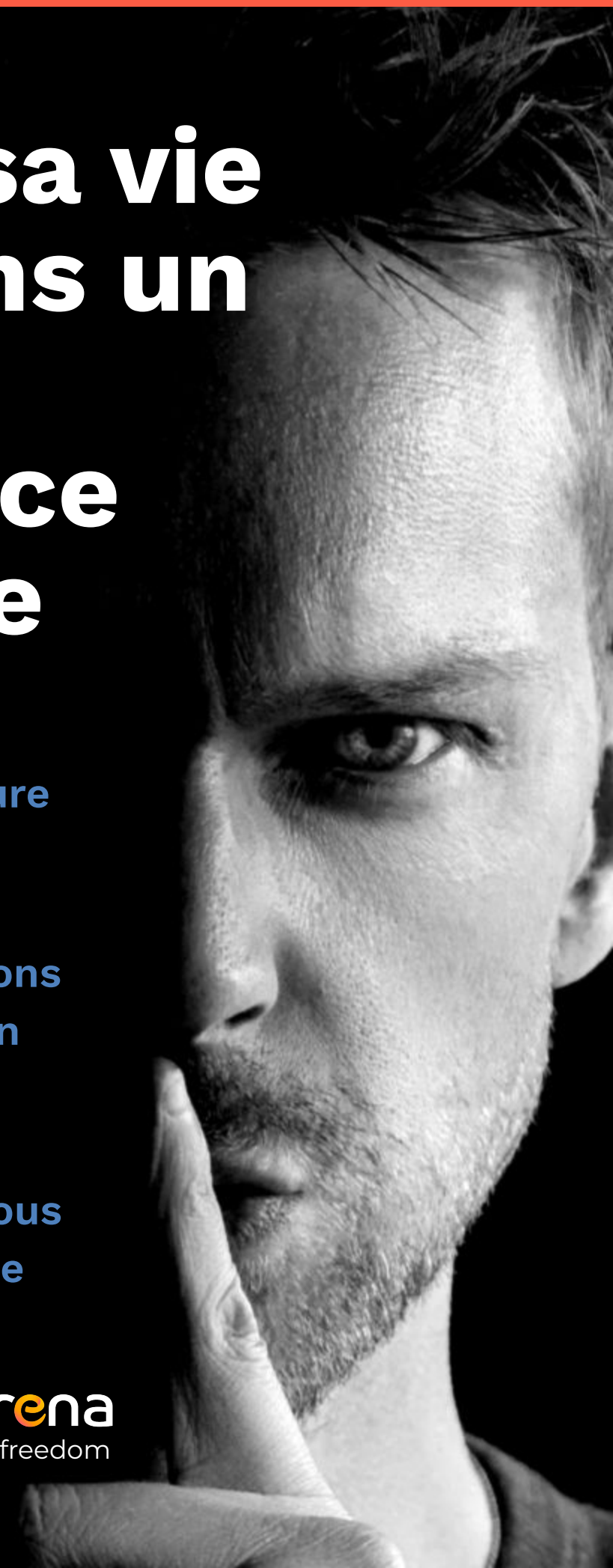
Protéger sa vie privée dans un monde de surveillance numérique

- Comment Google capture toute votre vie
- Comment les applications mobiles vous suivent en permanence
- 5 étapes faciles pour vous protéger, ainsi que votre famille

murena
choose freedom



En résumé

À l'ère numérique actuelle, la vie privée est devenue l'un des enjeux les plus cruciaux pour les individus et les sociétés. Les appareils sur lesquels nous comptons — notamment nos smartphones — collectent une immense quantité de données personnelles et professionnelles, souvent à notre insu ou sans véritable consentement.

Les géants de la technologie comme Google et Apple, ainsi qu'une vaste gamme d'applications mobiles, ont accès à des détails intimes de nos vies, et les méthodes qu'ils utilisent pour nous suivre posent des menaces importantes à notre vie privée et à notre sécurité.

Ce document explore jusqu'où vont les entreprises comme Google et Apple dans la collecte de données des utilisateurs, comment les applications mobiles suivent les utilisateurs via la publicité et les enchères en temps réel, ainsi que les conséquences potentielles de ces pratiques.
Il propose également des étapes faciles pour vous aider à vous protéger contre la surveillance numérique.

Comment Google collecte et utilise les données des utilisateurs

Google, l'une des plus grandes entreprises technologiques au monde, a bâti son empire en offrant des services "gratuits" comme Gmail, Google Search, YouTube et Google Maps tout en tirant d'immenses profits de la publicité. Cependant, ces services ont un coût important pour la vie privée des utilisateurs.

Comment Google collecte vos données :

- Suivi de localisation
- Historique de recherche et de navigation
- Communications personnelles
- Applications Google et Android

11,6 Mo/jour/utilisateur

Volume de données personnelles collectées par Google via les smartphones Android.

Source : Digital Content Next – Prof. Douglas C. Schmidt, Université Vanderbilt, août 2018.

Comment Google collecte et utilise les données des utilisateurs

Suivi de localisation

Google suit votre localisation, même lorsque vous n’utilisez pas Google Maps. Il collecte des données en temps réel à partir des appareils Android et peut déduire votre emplacement via des adresses IP, des réseaux Wi-Fi et des connexions Bluetooth.

Comment Google collecte et utilise les données des utilisateurs

Historique de recherche et de navigation

Chaque recherche effectuée sur Google Search et chaque site web visité via Google Chrome est suivi et enregistré. Cela permet à Google de constituer un profil détaillé de vos intérêts, habitudes et comportements.

Comment Google collecte et utilise les données des utilisateurs

Communications personnelles

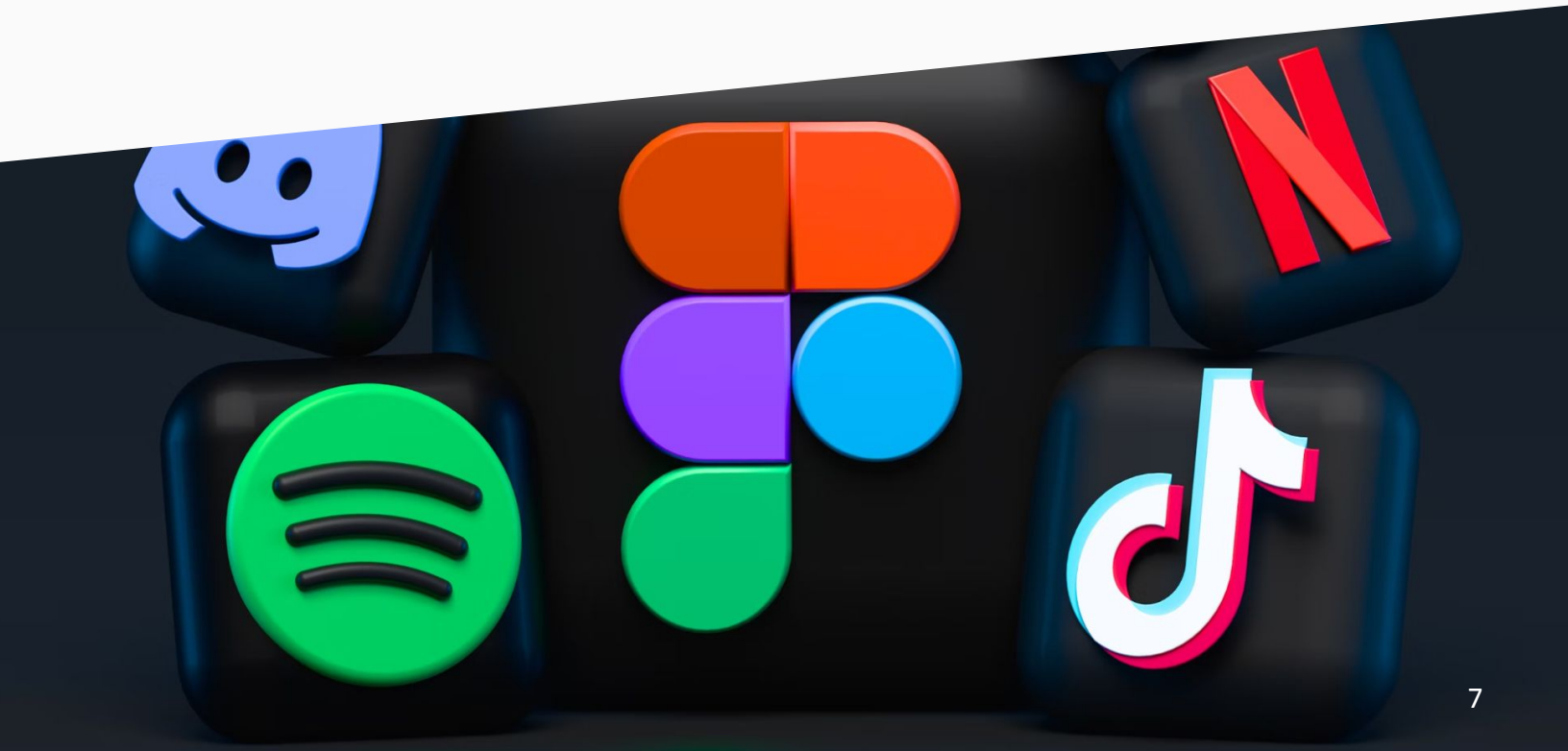
Si vous utilisez Gmail ou Google Drive, le contenu de vos emails et documents peut être scanné et analysé par les algorithmes de Google pour améliorer le ciblage publicitaire. Google collecte également les données des messages texte et des appels des utilisateurs Android sans consentement.

Source : "What Data Do The Google Dialer and Messages Apps On Android Send to Google?", Prof. Douglas Leith, Trinity College, Dublin, 2022.

Comment Google collecte et utilise les données des utilisateurs

Applications Google et Android

La plupart des téléphones Android sont liés à l'écosystème de Google, ce qui signifie que chaque interaction avec votre téléphone (comme l'ouverture d'applications, l'utilisation de l'appareil photo ou les commandes vocales) peut être collectée. Les services Google Play suivent comment et quand vous utilisez des applications et des sites web, donnant ainsi à Google un accès à des données comportementales étendues.



Approche d'Apple en matière de collecte de données

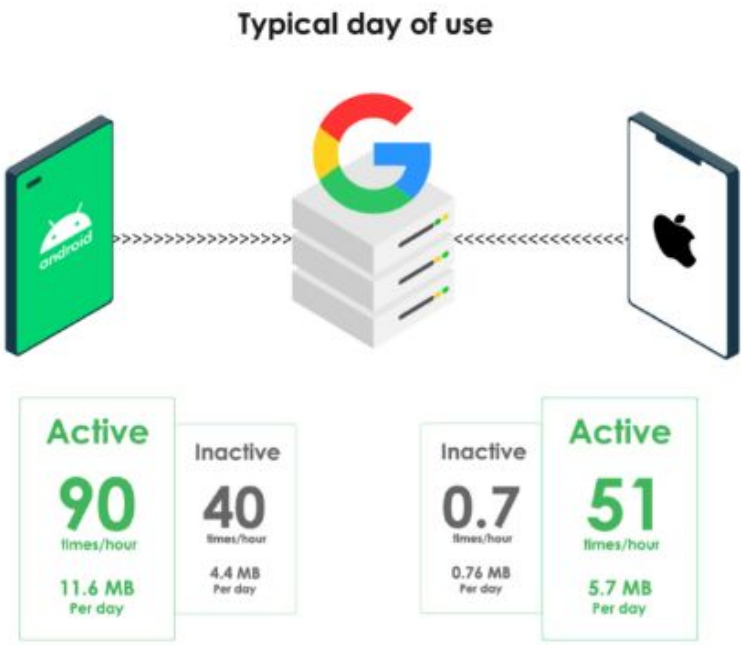
Bien qu'Apple se positionne comme une entreprise davantage axée sur la vie privée, elle participe également à une collecte significative de données. Apple ne collecte pas autant de données passivement que Google, mais elle en rassemble tout de même via ses services comme l'App Store, iCloud et Apple Health.

Apple reçoit également plus de 25 milliards de dollars par an de Google pour faire de Google Search le moteur de recherche par défaut sur les appareils iOS.

Volumes de données collectées :

- Un téléphone Android inactif transmet entre 4,4 Mo et 11,6 Mo de données personnelles par jour à Google.
- Un appareil Apple envoie entre 0,76 Mo et 5,7 Mo de données par jour à Google.

Source : Rapport de l'Université Vanderbilt.



Conséquences de la collecte de données par Google et Apple

Les efforts massifs de collecte de données de Google et Apple permettent à ces entreprises de constituer des profils extrêmement détaillés des individus, incluant leur historique de localisation, leurs recherches, leurs habitudes de communication et leurs achats en ligne. Cela soulève des préoccupations importantes en matière de vie privée :

- **Économie de surveillance :** Avec de telles données, Google (et des entreprises similaires) peut façonner nos expériences en ligne, limiter le contenu que nous voyons et manipuler nos décisions, que ce soit en matière d'achats, de préférences politiques ou de vie quotidienne.

- **Manipulation comportementale :** Avec des informations précises sur le comportement des utilisateurs, Google peut exploiter ses données pour influencer non seulement les publicités que les utilisateurs voient, mais potentiellement ce qu'ils pensent ou ressentent, mettant en péril leur autonomie.

- **Fuites de données :** Plus une entreprise collecte de données, plus elle devient une cible attrayante pour les pirates. Les violations de données chez des entreprises comme Google peuvent entraîner l'exposition d'informations personnelles.

Comment les applications mobiles utilisent la publicité et les enchères en temps réel pour suivre les utilisateurs

En dehors de Google et Apple, de nombreuses applications mobiles participent à des pratiques de suivi invasives à grande échelle, souvent sans que les utilisateurs en soient pleinement conscients. Comment les applications suivent les utilisateurs :

- **Identifiants publicitaires :** Les appareils mobiles disposent d'identifiants uniques, tels que l'IDFA (Identifier for Advertisers) d'Apple ou l'Advertising ID de Google, qui permettent aux applications de suivre les utilisateurs sur différentes plateformes. Ces identifiants sont utilisés pour diffuser des publicités ciblées.

- **Enchères en temps réel (RTB) :** RTB est un système d'enchères automatisé où les annonceurs enchérissent en temps réel pour afficher des publicités à des utilisateurs spécifiques. Lorsqu'une application ou un site web est ouvert, les annonceurs reçoivent immédiatement des informations sur l'utilisateur — comme sa localisation, son appareil et son comportement passé — et placent des enchères pour diffuser des publicités. Ce processus se produit des millions de fois par seconde.

Conséquences du suivi par les applications mobiles et des enchères en temps réel

Les données collectées par les applications mobiles et les enchères en temps réel posent de graves menaces à la vie privée des utilisateurs :

- **Manipulation ciblée :** Les données collectées via RTB permettent aux annonceurs de créer des publicités très ciblées et personnalisées. Bien que cela puisse améliorer la pertinence des publicités, cela permet également aux annonceurs (ou groupes politiques) de manipuler le comportement des utilisateurs en diffusant un contenu émotionnellement chargé.
- **Surveillance constante :** Les applications peuvent suivre votre localisation, votre utilisation des applications et votre comportement de navigation en temps réel, souvent sans votre consentement. Cela conduit à une surveillance continue de votre vie numérique.

- **Courtiers en données et érosion de la vie privée :** Les données collectées via RTB sont souvent partagées avec des courtiers en données tiers, qui peuvent compiler des profils complets sur les utilisateurs. Ces courtiers vendent vos données à des annonceurs, des gouvernements ou d'autres entités, ce qui aggrave encore l'érosion de votre vie privée.

Conseils pour vous protéger contre la surveillance numérique

Heureusement, plusieurs étapes peuvent être suivies pour vous protéger contre la surveillance numérique :

- **Désactiver le suivi de localisation :** Désactivez les services de localisation pour les applications qui n'en ont pas besoin et utilisez un VPN pour masquer votre adresse IP.
- **Bloquer les traceurs publicitaires :** Utilisez des extensions de navigateur axées sur la confidentialité. Désactivez les identifiants publicitaires sur Android et iOS. Le blocage des traceurs dans les applications et sur le web est également une fonctionnalité par défaut dans /e/OS.
- **Réduire les autorisations des applications :** Examinez régulièrement les autorisations des applications et révoquez l'accès aux données qui ne sont pas nécessaires au fonctionnement de base de l'application.
- **Utilisez des applications alternatives :** Remplacez autant que possible les applications et services Google, notamment Gmail et la recherche Google.
- **Utilisez le chiffrement de bout en bout :** Optez pour des applications de messagerie comme Signal, Matrix/Element ou Threema, qui offrent un chiffrement de bout en bout, garantissant que vos communications restent privées. Adoptez des services de messagerie électronique avec chiffrement de bout en bout complet, comme ProtonMail.
- **Envisagez des appareils axés sur la confidentialité :** Les smartphones Murena fonctionnant sous /e/OS sont conçus pour respecter votre vie privée en évitant les mécanismes de suivi de Google et les traceurs publicitaires.

La sécurité n'est PAS la vie privée !

Dans le paysage numérique actuel, il y a souvent confusion entre sécurité et vie privée. Bien que les deux soient essentiels, ils servent des objectifs différents :

- La sécurité vise à protéger les systèmes et les données contre tout accès non autorisé.
- La vie privée cherche à limiter la collecte et le partage de données personnelles dès le départ.

Un appareil peut être sécurisé tout en compromettant votre vie privée, car la sécurité ne prévient pas la collecte ou la surveillance de données par le propriétaire du système.

Exemples :

- **Spyware Pegasus sur iPhone :** Malgré la réputation des iPhones en matière de sécurité, des logiciels espions comme Pegasus ont exploité des failles pour pirater des cibles de haut niveau, y compris un président européen et des militants, sans interaction de l'utilisateur.
- **Hacking par la Russie des téléphones militaires :** Pendant le conflit en Crimée, les smartphones des soldats ukrainiens ont été piratés par les renseignements russes, permettant de suivre leurs mouvements et d'intercepter leurs communications, malgré l'utilisation de dispositifs cryptés de qualité militaire.
- **EncroChat et réseaux criminels :** Les téléphones cryptés utilisés par des réseaux criminels, comme EncroChat, ont été piratés par les forces de l'ordre européennes, conduisant à l'arrestation de nombreux criminels malgré leur réputation "d'immunité".

Comment Murena et /e/OS protègent votre vie privée

Contrairement aux principaux systèmes d'exploitation mobiles comme Android de Google et iOS d'Apple, /e/OS ne collecte pratiquement aucune donnée personnelle de ses utilisateurs. Selon une étude, /e/OS se distingue comme le système le plus respectueux de la vie privée parmi les diverses plateformes Android, telles que Samsung, Xiaomi et Huawei.

- **Pas de données envoyées à Google :** Contrairement aux autres variantes d'Android qui communiquent constamment avec les serveurs Google, /e/OS évite toute connexion avec les services Google. Cela empêche la collecte automatique de données sensibles comme l'historique de localisation, les recherches et l'utilisation de l'appareil.
- **Collecte minimale de données :** Les développeurs de /e/OS ont conçu le système pour fonctionner avec presque aucune transmission de données, même lorsque l'appareil est inactif. Aucune transmission d'identifiants de l'appareil, d'interactions de l'utilisateur ou de données d'utilisation des applications, une pratique courante sur d'autres variantes d'Android, n'a lieu.

Conclusion

Dans le monde numérique actuel, nos données personnelles sont de plus en plus collectées via des applications mobiles et des plateformes web. Les grands acteurs comme Google et Apple récoltent d'immenses quantités de données sur les utilisateurs, ce qui entraîne des risques significatifs à mesure que les comportements et préférences des utilisateurs sont suivis et vendus, souvent sans leur consentement éclairé.

Pour protéger votre vie privée :

- Désactivez le suivi de localisation et utilisez un VPN.
- Remplacez les services Google par des alternatives respectueuses de la vie privée.
- Préférez les applications de messagerie avec chiffrement de bout en bout.
- Envisagez des smartphones Murena fonctionnant sous /e/OS, conçus pour respecter votre vie privée.