« Les murs ont des oreilles... et votre voiture aussi ! »
Le constat est sans appel : tous les constructeurs automobiles passés en revue par Mozilla, y compris Ford, Volkswagen et Toyota, présentent d'importantes lacunes en termes de confidentialité

*La dernière édition du guide *Confidentialité non incluse de Mozilla révèle que 25 grands constructeurs automobiles recueillent et partagent des données parfois très personnelles pouvant porter sur l'activité sexuelle, les expressions faciales, mais aussi le patrimoine génétique ou encore la santé des conducteurs-trices.*

(MERCREDI 6 SEPTEMBRE 2023) — Les 25 grands constructeurs automobiles passés au crible dans la dernière édition du guide *Confidentialité non incluse de Mozilla ont tous obtenu des notes insuffisantes en ce qui concerne la protection des données de leurs clients : du jamais vu depuis le lancement du guide d'achat il y a sept ans !

Attachez votre ceinture : la dernière étude de Mozilla révèle que des constructeurs automobiles connus et vendus dans le monde entier comme **BMW, Ford, Toyota, Tesla, Kia** et **Subaru** peuvent recueillir des données très personnelles concernant par exemple l'activité sexuelle, la situation en termes d'immigration, l'origine ethnique, les expressions faciales, le poids, l'état de santé et le patrimoine génétique, ainsi que des informations sur les trajets effectués. Les chercheurs ont découvert que toutes ces données sont recueillies par le biais de capteurs, de microphones, de caméras, mais aussi par les téléphones et les appareils connectés aux véhicules, ainsi que les applications automobiles, les sites web des entreprises, les concessionnaires et enfin par les équipements [téléométriques](#) des [véhicules](#). Les constructeurs peuvent ensuite partager ou vendre ces données à des entreprises tierces ou les utiliser pour établir des profils en faisant des déductions sur l'intelligence, les capacités, les caractéristiques et les préférences des conducteurs-trices.

Pour couronner le tout, aucun des constructeurs ne répond aux [exigences de sécurité minimales établies par Mozilla](#). Ainsi, les chercheurs n'ont même pas été en mesure de confirmer si *au moins une* des marques automobiles chiffrait bien les informations

personnelles stockées dans les véhicules, et seule **Mercedes** a daigné répondre aux questions de Mozilla à ce sujet.

La dernière édition de *Confidentialité non incluse s'est penchée sur les failles en matière de confidentialité et de sécurité des marques automobiles provenant de cinq pays : les États-Unis, l'Allemagne, le Japon, la France et la Corée du Sud. Les chercheurs ont consacré 600 heures à lire les politiques de confidentialité, à télécharger des applications et à correspondre avec les marques ; la méthodologie complète peut être consultée [ici](#).

Autant le dire tout de suite : c'est du côté de **Nissan** que la situation est la plus alarmante. Le constructeur automobile japonais reconnaît dans sa politique de confidentialité recueillir un large éventail d'informations, notamment des données sur l'activité sexuelle, les diagnostics médicaux et le patrimoine génétique de ses client·e·s, sans toutefois préciser *comment*. Nissan indique également qu'elle peut partager et vendre les « préférences, caractéristiques, tendances psychologiques, prédispositions, comportements, attitudes, intelligence, capacités et aptitudes » de ses client·e·s à des courtiers en données, aux autorités ainsi qu'à d'autres tiers (tant qu'à faire !).

Mais les autres marques ne sont pas en reste. **Volkswagen** recueille des données démographiques (comme l'âge et le sexe des conducteurs·trices) ainsi que leurs comportements sur la route (comme leur utilisation ou non de la ceinture de sécurité ou leurs habitudes de freinage) dans le but d'affiner le ciblage de ses campagnes marketing. **Toyota**, pour sa part, détaille sa politique de confidentialité dans pas moins de 12 documents différents. Quant à **Kia**, la marque coréenne affirme sans rougir qu'elle peut recueillir des informations sur la « vie sexuelle » de ses client·e·s, ce qui n'est pas sans susciter quelques inquiétudes. Enfin, **Mercedes-Benz** va jusqu'à préinstaller TikTok (qui traîne déjà ses propres casseroles en matière de confidentialité) sur certains de ses modèles. Les analystes [estiment](#) que d'ici 2030, la monétisation des données automobiles pourrait représenter jusqu'à 750 milliards de dollars.

Malheureusement (ou plutôt naturellement), aucune marque n'a pu recevoir le label « Meilleur choix » décerné par Mozilla. Cependant, les chercheurs ont désigné **Renault** comme étant la moins problématique. Cette marque française (cocorico !) doit en effet se conformer au Règlement général sur la protection des données, communément appelé RGPD, régissant la manière dont les données personnelles sont utilisées, traitées et stockées au sein de l'Union européenne.

Jen Caltrider, la directrice du programme *Confidentialité non incluse, n'est pas surprise : « Beaucoup de gens considèrent leur voiture comme un espace privé, où ils peuvent appeler leur médecin, avoir une conversation privée avec leur enfant en allant à l'école, pleurer après une rupture ou se rendre dans des endroits qu'ils ne souhaitent peut-être pas rendre publics. Cette perception ne correspond plus à la réalité. Toutes les voitures neuves d'aujourd'hui sont de véritables cauchemars sur roues en matière de confidentialité, qui collectent d'énormes quantités d'informations personnelles. »

Misha Rykov, chercheur au sein du programme *Confidentialité non incluse, tire également la sonnette d'alarme : « Ce n'est pas la première fois que Mozilla lève le voile sur un secteur aux pratiques de confidentialité déplorables. Mais les voitures sont un cas à part : leurs failles en matière de confidentialité affectent non seulement le·a conducteur·trice, mais aussi les passagers·ères et parfois même les piétons à proximité. Elles peuvent vous entendre, vous voir et vous suivre. Aujourd'hui, s'asseoir dans la voiture de quelqu'un revient presque systématiquement à remettre son téléphone au constructeur automobile. ».

Voici d'autres conclusions notables de l'étude :

- **Les applications apportent un niveau de complexité supplémentaire.** De nos jours, rares sont les produits qui ne bénéficient pas d'une application dédiée, et les automobiles ne font pas exception. Les voitures disposent aujourd'hui d'applications qui peuvent s'avérer pratiques pour vous aider à retrouver votre véhicule dans un parking ou même à le démarrer à distance. Malheureusement, ces mêmes applications sont également un moyen de recueillir encore plus de données... De plus, la gouvernance de ces applications pose parfois question : **BMW** USA gère par exemple une application pour le compte de **Toyota**.
- **De nombreux constructeurs automobiles se livrent au « Privacy Washing »,** une pratique qui consiste à faire semblant de protéger la vie privée des consommateurs·trices sans intention de le faire réellement. Plusieurs constructeurs de notre étude ont par exemple adhéré aux [Principes de protection de la vie privée des consommateurs·trices](#) dans le secteur automobile. Mais ces principes ne sont absolument pas contraignants et ont été *créés par les constructeurs automobiles eux-mêmes*. Enfin, comble de l'ironie, les signataires ne respectent même pas leurs propres principes, comme la minimisation des données (c'est-à-dire collecter uniquement les données qui sont nécessaires).

- **D'importantes lacunes existent** en termes de consentement. Et dans la plupart des cas, il suffit d'être passager·ère dans un véhicule pour que celui-ci soit présumé. **Subaru** affirme par exemple que dès lors que vous êtes passager·ère, vous êtes considéré·e comme un·e utilisateur·trice, et qu'en tant que tel·le, vous avez implicitement accepté sa politique de confidentialité. D'autres constructeurs automobiles précisent également que c'est au·à la conducteur·trice qu'incombe la responsabilité d'informer les passagers·ères des politiques de confidentialité du véhicule.
- **Les politiques de confidentialité et les pratiques en la matière dans le secteur automobile laissent particulièrement à désirer.** Les politiques de confidentialité claires sont déjà rares en temps normal, mais elles le sont encore moins ici. De grandes marques comme **Audi** et **Tesla** proposent des politiques de confidentialités vagues, longues et confuses. D'autres possèdent pas moins de cinq documents de politique de confidentialité différents, et **Toyota** en compte même 12. Par ailleurs, il est difficile, pour ne pas dire impossible, de contacter un interlocuteur pour parler de ce sujet : 12 entreprises représentant 20 marques automobiles n'ont même pas répondu aux e-mails envoyés par les chercheurs de Mozilla.
- **Les constructeurs automobiles partagent des informations personnelles avec les forces de l'ordre et les gouvernements. La politique de confidentialité de Hyundai**, par exemple, précise que la marque peut communiquer des données avec les forces de l'ordre et les gouvernements en fonction de demandes « formelles ou informelles » qu'elle reçoit. La politique de **Kia** précise que le constructeur peut transmettre des données dans de nombreux scénarios, par exemple, « si, selon notre bonne foi, cela est requis ou permis par la loi ». Autant dire que les critères retenus pour partager des informations extrêmement sensibles sont *très* larges.
- **Les fuites de données sont courantes.** Des fuites de données graves surviennent fréquemment dans le secteur automobile. On peut citer par exemple le cas des employé·e·s **Tesla** qui regardent des vidéos enregistrées par les voitures des client·e·s ou encore celui des millions de client·e·s **Volkswagen** et **Toyota**, dont les informations personnelles se sont retrouvées dans la nature (ou disons plutôt à la merci des hackers sur Internet).

- **Les consommateurs·trices disposent de très peu de moyens de contrôle.** Les client·e·s de ces grands constructeurs de véhicule pourraient choisir de ne pas utiliser l'application automobile ou les services connectés du constructeur. Mais cela impliquerait que leur voiture ne fonctionne pas correctement, voire pas du tout dans certains cas. En ce qui concerne le respect de leur vie privée, les consommateurs·trices n'ont presque aucun moyen de contrôle ni choix à exercer, à moins d'opter tout simplement pour un modèle plus ancien. Les régulateurs et les décideurs politiques accusent un retard important sur ce front.

À propos du guide *Confidentialité non incluse

*Confidentialité non incluse est un guide d'achat axé sur la confidentialité plutôt que sur le prix ou les performances techniques. Lancé en 2017, ce guide a passé en revue des centaines de produits et d'applications. Il fournit aux acheteur·euse·s les informations nécessaires pour protéger la vie privée de leurs amis et de leur famille, tout en encourageant les acteurs du secteur technologique à faire davantage pour protéger les consommateurs·trices.