

DOCUMENT CONJOINT DES AUTORITÉS DE PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE DU G7 SUR LES APPAREILS DOMESTIQUES CONNECTÉS ET LA VIE PRIVÉE DES ENFANTS

INTRODUCTION

Nous les autorités de protection des données et de la vie privée (APD) du G7, reconnaissons l'impact croissant que les appareils domestiques connectés tels que les téléviseurs connectés, les assistants vocaux virtuels et d'autres appareils connectés à internet, tels que les jouets connectés, ont sur la vie quotidienne des personnes, en particulier les enfants.

Nous sommes conscients que ces produits et appareils ont la capacité de déployer des technologies de suivi en ligne. Les fabricants et les parties prenantes de l'industrie utilisent des technologies de suivi en ligne, y compris les cookies, les pixels de suivi, les ETags, l'empreinte numérique des appareils ou la reconnaissance automatique de contenu (ACR), pour collecter et stocker les données d'une personne lorsqu'elle utilise des appareils domestiques connectés compatibles avec internet. Dans certains cas, ces processus pourraient avoir lieu sans que la personne concernée ne sache qu'un tel traitement de données a lieu.

Nous reconnaissons que les appareils domestiques connectés peuvent apporter des avantages avec la possibilité pour les individus d'avoir des expériences plus personnalisées ou d'accroître l'accessibilité. Dans le même temps, ces appareils sont généralement conçus pour être utilisés dans des endroits où les individus ont les plus grandes attentes en matière de vie privée : le foyer. L'utilisation de technologies de suivi en ligne dans ces appareils domestiques connectés permet de surveiller les activités et les comportements quotidiens des propriétaires d'appareils, ainsi que ceux des personnes vivant avec le propriétaire de l'appareil ou visitant le domicile du propriétaire de l'appareil. Grâce à cette surveillance, les appareils domestiques connectés peuvent être en mesure de collecter et de révéler des informations sur des personnes, y compris des enfants, à grande échelle.¹

Les données issues² d'études de consommateurs, des plaintes auprès des régulateurs et des articles de recherche³ mettent en évidence une série de risques potentiels pour la protection des données et la vie privée associés aux appareils domestiques connectés, en particulier lorsqu'ils sont utilisés par des enfants, qui peuvent être moins conscients des conséquences du traitement de leurs données à caractère personnel.

CONSIDÉRATIONS RELATIVES À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE DES ENFANTS POUR DES PRATIQUES RESPONSABLES

¹ [Les marques d'appareils intelligents récoltent vos données - Lesquelles?](#)

² [Rapport du jury citoyen sur l'internet des objets – Bureau du commissaire à l'information](#)

³ [L'Internet des objets - Introduction aux questions de protection de la vie privée en mettant l'accent sur les environnements du commerce de détail et de la maison - Commissariat à la protection de la vie privée du Canada](#)

Des considérations particulières sont nécessaires pour les appareils domestiques connectés qui ciblent spécifiquement les enfants, traitent les informations des enfants ou sont susceptibles d'être accessibles aux enfants. Nous encourageons les fabricants, les fournisseurs de logiciels et les entreprises de l'écosystème de suivi en ligne à veiller à ce que ces appareils domestiques connectés respectent, en particulier, les principes suivants:

1. Confidentialité dès la conception et par défaut – Les paramètres de géolocalisation et de publicité comportementale en ligne devraient être désactivés par défaut et les appareils devraient être conçus de manière à réduire au minimum la collecte de données par défaut. Les paramètres par défaut pour des fonctionnalités telles que le profilage comportemental pour le contenu ou les recommandations d'amis, la création de compte et le partage de données devraient être désactivés ou réglés au niveau de confidentialité le plus élevé possible afin d'éviter le traçage des comportements des enfants et de renforcer la protection contre l'accès à des contenus inappropriés et les interactions avec des étrangers.
2. Transparence claire et accessible – Veiller à ce que la politique de confidentialité et toutes les autres communications, y compris les conditions d'utilisation, soient claires et utilisent un langage facilement compréhensible, adapté au niveau de maturité de l'enfant. Une telle communication devrait être visible, en particulier lorsque l'appareil n'a pas d'écran. Les informations sur la transparence devraient être fournies dans des éléments plus petits et faciles à comprendre, et à un endroit et à un moment appropriés lorsque des décisions sont nécessaires. Il conviendrait de réfléchir davantage à l'utilisation de formats créatifs, tels que les vidéos, pour fournir ces informations aux différents groupes d'âge, et à la manière dont les informations sur la transparence sont fournies lorsqu'il n'y a pas d'interface d'écran sur un appareil. Une notice appropriée devrait également être fournie aux parents.
3. Mécanismes de consentement valides – Fournir des outils de protection de la vie privée et des mécanismes de consentement adaptés aux enfants et à leur degré de maturité (ou, le cas échéant ou si la loi l'exige, le consentement de leur parent/tuteur). Les appareils domestiques connectés ne devraient pas utiliser des modèles de conception trompeurs pour encourager l'enfant à fournir plus d'informations qu'il n'est raisonnablement nécessaire pour accéder au service. Les mécanismes de consentement devraient également tenir compte de l'évolution des capacités de l'enfant.
4. Contrôle et choix de l'utilisateur – Les enfants et/ou leurs parents/tuteurs devraient avoir des choix significatifs s'agissant de savoir si et comment leurs données sont collectées et utilisées, y compris des options claires et affichées de manière visible sur l'appareil pour accepter ou refuser le traitement des données, et pour gérer leurs choix sur une base continue.
5. Traitement licite et loyal des données – Comprendre le risque élevé associé au traitement des données des enfants et l'importance de procéder à des évaluations appropriées⁴ pour identifier les dommages et les risques spécifiques aux enfants et leur vulnérabilité. S'assurer qu'une base légale pour le traitement s'applique à l'appareil et au service.

⁴ [Exemple d'analyse d'impact relative à la protection des données : Jouet connecté](#)

6. Éviter la collecte passive de données – Les appareils domestiques connectés qui peuvent «écouter» ou enregistrer des données devraient notifier ou divulguer de manière visible lorsqu'ils collectent des données à caractère personnel, afin que les enfants et/ou leurs parents/tuteurs soient informés afin qu'ils puissent exercer de manière significative leurs droits quant à la méthode et à l'utilisation de leurs données.
7. Conservation des données - Les données des enfants collectées légalement ne doivent pas être conservées plus longtemps que nécessaire aux fins pour lesquelles elles sont traitées, ou pour se conformer aux exigences légales.
8. Mesures de sécurité fortes – Compte tenu de la sensibilité accrue des données à caractère personnel des enfants, les entreprises devraient veiller à ce que des mesures de sécurité robustes soient mises en place par défaut, y compris la mise à jour automatique et régulière des logiciels, en fournissant aux utilisateurs un contrôle et des connaissances suffisants sur les paramètres de sécurité et en empêchant les accès non autorisés, les violations de données ou l'utilisation abusive de données à caractère personnel.
9. Responsabilité tout au long de la chaîne d'approvisionnement – Les fabricants et les prestataires de services devraient assumer la charge de garantir la responsabilité dans l'ensemble de l'écosystème de données lors du partage de données, en particulier lorsqu'ils travaillent avec des fournisseurs tiers ou dans d'autres cas où les fabricants et les prestataires de services risquent de manquer de contrôle sur les mesures de sécurité utilisées par exemple.
10. L'intérêt supérieur de l'enfant – Les fabricants devraient examiner la manière dont les enfants sont susceptibles d'interagir avec l'appareil domestique connecté et envisager d'autres besoins ou exigences en matière de protection de la vie privée afin de veiller à ce que les appareils soient développés de manière à se conformer à la politique ou à la législation applicable des juridictions concernées.