

GÉRER VOTRE VIE PRIVÉE LORSQUE VOUS UTILISEZ DES APPAREILS INTELLIGENTS

Aujourd'hui, il n'y a pas que les ordinateurs ou même les téléphones qui se connectent à Internet : il y a de fortes chances que vous ayez un ou plusieurs appareils « intelligents » à la maison.

Qu'il s'agisse d'une sonnette vidéo, d'un assistant vocal intégré à un haut-parleur, ou même de « chaussettes intelligentes » pour votre bébé, toutes ces choses ont un point commun : elles utilisent des données pour fonctionner. Parfois, ces données sont personnelles. Vous devez donc savoir comment les gérer.

Le type et la *quantité* de données recueillies dépendent de vous, du moins en partie. Voici quelques mesures que vous pouvez prendre pour gérer votre vie privée lorsque vous utilisez des appareils intelligents.

Préoccupez-vous de votre vie privée lorsque vous magasinez. Certains appareils recueillent plus ou moins de données que d'autres. Par exemple, certaines sonnettes intelligentes ne stockent les vidéos que localement (sur un disque dur ou une carte mémoire) plutôt que de les télécharger sur le nuage informatique. (N'oubliez pas que nous ne devons pas seulement nous préoccuper de notre vie privée, mais nous devons aussi respecter celles des *autres*.) Il est important de vérifier ces fonctionnalités, y compris les options de stockage des données disponibles comme la suppression et le chiffrement.

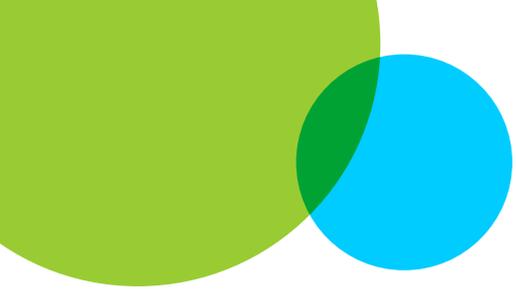
Avant de prendre votre décision, il est important de lire la politique de confidentialité. Elle précise les données que l'entreprise recueille, ce qu'elle en fait, ainsi que les droits et les options dont vous disposez pour les contrôler.

Le site *Web Terms of Service, Didn't Read* (www.tosdr.org/) résume et évalue les conditions

d'utilisation et les politiques de protection de la vie privée.

Vous pouvez également consulter vous-même la politique de protection de la vie privée avant de décider de votre achat. Il est plus facile de le faire sur un ordinateur portable ou de bureau : le texte y est plus facile à lire et vous pouvez utiliser la touche Ctrl+F pour rechercher des mots clés.

- Recherchez les dérivés du mot « recueillir » comme dans « les données que nous recueillons » ou « façon dont nous recueillons et utilisons vos données ». Vous pouvez ouvrir un nouvel onglet afin de rechercher les mots que vous ne reconnaissez pas ou que vous n'êtes pas sûr de connaître, comme « biométrique » ou « géolocalisation ».
- Recherchez les mots « partenaires » et « partager » ou l'expression « tiers ». Vous saurez ainsi avec quelles *autres* entreprises vos données peuvent être partagées (ou à qui elles peuvent être vendues).
- Recherchez l'expression « façon dont nous utilisons ». Cette section vous expliquera les différentes utilisations que l'entreprise fera de vos données. Il peut être difficile de savoir quel effet cette pratique aura sur vous. Par exemple, les données sur votre santé provenant d'un appareil portable peuvent influencer le montant de votre assurance et donc, si cette partie de la politique n'est



GÉRER VOTRE VIE PRIVÉE LORSQUE VOUS UTILISEZ DES APPAREILS INTELLIGENTS

pas claire ou si elle ne vous convient pas, envisagez alors une autre option.

- Recherchez des mots comme « droits » ou « choix ». Ces conditions vous expliqueront vos droits en matière de protection de la vie privée en vertu de la loi (assurez-vous de lire la section correspondant à votre lieu de résidence) et peuvent également vous indiquer de quelle façon vous pouvez demander à voir les données qui ont été recueillies ou à les faire supprimer, ou vous désister de certaines des méthodes utilisées par l'entreprise pour recueillir et utiliser vos données.

Apprenez à connaître l'application. La plupart des appareils intelligents n'ayant pas d'écran, ils sont presque tous dotés d'une application que vous installez sur votre téléphone ou tablette. L'application permet de modifier les différents paramètres de l'appareil. Un grand nombre des suggestions ci dessous traite de la modification de ces paramètres. Il est donc utile de se familiariser avec l'application et la manière de l'utiliser.

Toutefois, l'installation de l'application permet également à l'entreprise qui fabrique l'appareil d'accéder à certaines données sur votre téléphone ou tablette. Certaines applications recueillent des données lorsque vous les utilisez, et d'autres recueillent les mêmes données lorsque vous utilisez *d'autres* applications sur le même appareil. Voici comment y mettre fin.

- Si vous avez un iPhone ou un iPad, choisissez l'option « Demander à l'app de ne pas faire de suivi » lorsque vous installez une application.

Si vous avez déjà installé des applications pour appareils intelligents, allez dans les réglages, puis dans l'option « Confidentialité et sécurité » et ensuite dans « Suivi ». Recherchez l'application et désactivez l'option « Autorisation du suivi par les apps ».

- Si vous avez un appareil Android, installez l'application DuckDuckGo. Allez dans les réglages, puis activez la protection contre le suivi des applications.
- Si vous utilisez un ordinateur portatif ou de bureau pour contrôler votre appareil, assurez-vous que votre navigateur dispose d'une extension telle que Privacy Badger ou Ghostery qui bloque la collecte de données.

Toute personne ayant accès à l'application peut également modifier les paramètres de l'appareil. Pensez donc à installer des applications pour appareils intelligents sur une tablette ou un vieux téléphone qui ne quitte jamais la maison. Ainsi, vous n'aurez pas à craindre que quelqu'un qui le trouve ou le vole ait accès à l'appareil.

Passez en revue les paramètres de confidentialité. Une fois que vous vous êtes familiarisé avec l'application, recherchez les paramètres de confidentialité. Il s'agit généralement d'une option dans la section principale des réglages, mais si vous avez de la difficulté à les trouver, vous pouvez utiliser un moteur de recherche et chercher « Paramètres de confidentialité » en plus du nom de votre appareil (p. ex. « paramètres de confidentialité Alexa »).

Les paramètres de confidentialité varient d'un appareil à l'autre. Voici quelques options que vous pouvez

envisager. (Si vous magasinez un appareil intelligent, tentez de savoir lesquelles de ces options sont proposées sur l'appareil.)

- *Désactivez la collecte et le partage de données.* Presque tous les appareils intelligents envoient des données aux entreprises, lesquelles utilisent ces données à des fins très diverses, comme pour améliorer le fonctionnement du service ou envoyer des publicités ciblées. Il est possible que vous puissiez refuser que vos données soient recueillies ou utilisées à ces fins. Par exemple, sur un appareil Alexa, accédez à l'option de confidentialité, puis choisissez l'option de gestion de vos données Alexa. Vous pouvez également refuser de recevoir des publicités personnalisées sur Amazon [ici](#).
- *Supprimez votre historique.* Les appareils intelligents enregistrent souvent ce que vous avez fait avec eux dans le passé, comme des choses précises que vous avez dites à un haut-parleur intelligent en utilisant le mot d'activation (plus de détails sur le sujet ci-dessous). Vous pouvez revoir ce qui a été enregistré, en supprimer une partie ou la totalité, et mettre l'historique en pause pour éviter qu'il n'enregistre des données à l'avenir en sélectionnant l'option « Ne pas sauvegarder les enregistrements », ou une option semblable.
- *Modifiez le mot de passe et le mot d'activation.* La plupart des appareils intelligents sont livrés sans mot de passe ou sont dotés d'un mot de passe par défaut. Trouvez un mot de passe fiable. (Consultez notre courte vidéo à l'adresse <https://www.youtube.com/bonmotdepasse> pour obtenir des conseils rapides sur la création d'un bon mot de passe.)

- Les haut-parleurs intelligents sont également dotés d'un mot d'activation qui leur commande de commencer à vous écouter. Pour vous assurer que l'appareil ne s'activera pas par accident, modifiez le mot d'activation. (Les haut-parleurs intelligents ne permettent pas tous de modifier le mot d'activation. D'autres proposent une gamme limitée d'options de mots d'activation. Choisissez donc celui qui vous convient le mieux.) Si vous parlez une autre langue que le français, vous pourrez peut-être configurer votre haut-parleur pour qu'il entende et réponde dans cette langue.
- S'il est possible d'acheter quoi que ce soit sur l'appareil, assurez-vous que cette option est également désactivée. (Ainsi, les autres membres de votre foyer ne pourront pas acheter quelque chose par accident.)

Si l'appareil est lié à votre compte auprès d'une entreprise comme Google, Apple ou Amazon, vous pouvez également modifier certains paramètres dans votre compte principal. Par exemple, si vous ne souhaitez pas que votre haut-parleur intelligent Amazon diffuse des publicités ciblées, vous pouvez désactiver les publicités axées sur vos intérêts sur la page des préférences publicitaires d'Amazon. (L'appareil diffusera tout de même des publicités, mais elles ne seront pas fondées sur vos données personnelles.)

Créez un compte d'invité sur votre réseau Wi-Fi. En ne connectant pas l'appareil sur votre compte Wi-Fi principal, vous limitez ainsi également les données qui peuvent être recueillies. Votre fournisseur d'accès



GÉRER VOTRE VIE PRIVÉE LORSQUE VOUS UTILISEZ DES APPAREILS INTELLIGENTS

Internet vous a peut-être fourni une application qui vous permet de modifier les paramètres de votre routeur. Si c'est le cas, il devrait y avoir une option permettant de créer un réseau d'invités. Dans le cas contraire, communiquez avec votre fournisseur d'accès à Internet pour lui demander de l'aide.

Désactivez les micros et les caméras lorsque vous n'en avez pas besoin. Bon nombre d'appareils intelligents dotés de micros ou de caméras disposent d'interrupteurs physiques ou d'options dans l'application pour les éteindre (p. ex. les appareils Alexa disposent d'un bouton de sourdine sur le dessus et indiquent par une lumière rouge que l'appareil est en mot muet. Vous obtiendrez le même résultat en disant simplement « Alexa, arrête l'enregistrement ».)

Couvrez également les caméras lorsque vous ne les utilisez pas. La plupart des appareils intelligents dotés d'une caméra disposent d'un voyant qui s'allume

lorsque la caméra est active, mais pour plus de sécurité, vous devriez placer une note autocollante ou quelque chose de similaire sur tout appareil intelligent dont la caméra n'a pas besoin d'être allumée en permanence.

N'oubliez pas les applications supplémentaires. Certains appareils intelligents sont dotés d'applications supplémentaires ou de « capacités » qui leur permettent de faire différentes choses. Certaines de ces applications sont créées par des entreprises différentes de celle qui a fabriqué l'appareil et peuvent recueillir des données différentes ou les utiliser à d'autres fins. Ne téléchargez des applications qu'à partir de la boutique officielle de l'appareil et vérifiez la politique de confidentialité avant d'installer une nouvelle application ou « capacité ».

