Enceintes intelligentes : des assistants vocaux connectés à votre vie privée

05 décembre 2017

Guidée vocalement, une enceinte connectée assiste l’utilisateur dans les tâches de son quotidien.

Quels enjeux posent cette technologie au regard de la vie privée des utilisateurs ?

# Qu’est-ce qu’une enceinte connectée dite « intelligente » ?

Une enceinte connectée « intelligente » est un dispositif équipé d’un haut-parleur et d’un micro qui intègre un assistant vocal.

Grâce à cet équipement, l’enceinte est capable d’interagir avec l’utilisateur pour lui délivrer un service suite à une requête vocale.

L’assistant est en mesure de répondre à une question, donner la météo, régler le chauffage, activer des lumières, réserver un VTC/Taxi, acheter des billets …

Le principe général de fonctionnement se caractérise par 4 grandes étapes :

## Etape 1 - L’utilisateur « réveille » l’enceinte à l’aide d’une expression clé (« Hey Snips » / « Ok Google » / « Hey Alexa »).

L’enceinte est en permanence à l’écoute du mot clé mais n’enregistre rien et ne procède à aucune opération tant qu’elle ne l’a pas entendu.

## Etape 2 – L’utilisateur énonce sa requête.

Certaines de ces enceintes enregistrent localement les requêtes de l’utilisateur de manière à lui laisser la maitrise de ses données (ex. une enceinte connectée avec l’assistant vocal de Snips). D’autres en revanche, envoient ces requêtes dans le cloud, autrement dit sur les serveurs de traitement de la société (ex. Amazon Echo, Google Home,…). Dans les deux cas, l’appareil (ou ses serveurs) peut être amené à conserver :

Un historique des requêtes transcrites afin de permettre à la personne de pouvoir les consulter et à l’éditeur d’adapter les fonctionnalités du service.

Un historique des requêtes audio afin de permettre à la personne de les réécouter et à l’éditeur d’améliorer ses technologies de traitement de la parole.

Les métadonnées associées à la requête comme par exemple, la date, l’heure, le nom du compte…

## Etape 3 – La parole prononcée est automatiquement transcrite en texte puis interprétée afin qu’une réponse adaptée soit fournie.

Une phrase de réponse est synthétisée puis jouée sur l’enceinte et/ou une commande est passée (monter les stores, augmenter la température, jouer un morceau de musique, répondre à une question, etc.)

## Etape 4 - L’enceinte repasse en « veille »

# Assistants vocaux : bien comprendre les enjeux autour de votre vie privée

D’abord déployés sur les téléphones, puis les enceintes ou les casques audio, les assistants à commande vocale sont amenés à progressivement s’intégrer dans l’habitacle de votre véhicule, à l’intérieur d’un robot domestique, et même sur votre lieu de travail. Chaque utilisateur doit ainsi intégrer que même si « la parole s’envole », ses requêtes vocales sont enregistrées dans le cloud, de la même manière qu’elles le seraient s’il les tapait au clavier dans certains moteurs de recherche !

Un point de vigilance qui s’ajoute aux diverses interrogations auxquelles vous serez peut-être un jour confronté en tant qu’utilisateur, notamment sur :

## La confidentialité des échanges

En veille permanente, ces assistants sont susceptibles d’enregistrer vos conversations, y compris celles de tiers lorsqu’ils ont reconnu le mot clé.

Nos conseils

Encadrer les interactions de ses enfants avec ce type d’appareils (rester dans la pièce, éteindre le dispositif lorsqu’on n’est pas avec eux) ;

Couper le micro / éteindre l’appareil lorsque l’on ne s’en sert pas où lorsqu’on ne souhaite pas pouvoir être écouté ;

Avertir des tiers/invités de l’enregistrement potentiel des conversations (ou couper le micro lorsqu’il y a des invités)

Vérifier qu’il est bien réglé par défaut pour filtrer les informations à destination des enfants.

## La monétisation de l’intime

Principalement destinées au domicile pour contrôler des objets connectés et des services de divertissement, les appareils dotés d’un assistant à commande vocale se retrouvent au cœur de la vie du foyer.

Nos conseils

Connecter des services qui présentent réellement une utilité pour vous, tout en considérant les risques à partager des données intimes ou des fonctionnalités sensibles (ouverture porte, alarme…) ;

Etre vigilant sur le fait que les propos tenus face à l’appareil peuvent enrichir votre profil publicitaire ;

Ne pas hésiter à contacter les services supports en cas de questions et, le cas échéant, la CNIL.

## L’absence d’écran

L’individu échange vocalement avec un assistant connecté sans nécessairement s’appuyer sur un tableau de bord visuel. Sans écran, difficile d’avoir un aperçu des traces enregistrées, ni de juger de la pertinence des suggestions, d’en savoir plus ou d’avoir accès à des réponses provenant d’autres sources.

Notre conseil

Se rendre régulièrement sur le tableau de bord pour supprimer l’historique des conversations/questions posées et personnaliser l’outil selon vos besoins. Par exemple, définir le moteur de recherche ou la source d’information utilisé par défaut par l’assistant;

# Quel encadrement de la gestion des données des utilisateurs ?

La CNIL est en contact avec les différents fabricants afin d’avoir une parfaite compréhension des systèmes déployés. Elle réalise des tests sur certains de ces appareils et mène des réflexions sur les moyens à mettre en œuvre afin de garantir que les utilisateurs sont bien informés des données collectées, des usages qui en sont faits et des moyens à leur disposition pour y accéder, les modifier, les supprimer, etc.