

Pourquoi Edward Snowden déconseille Allo, la nouvelle messagerie de Google



Le lanceur d'alerte à l'origine du scandale de la surveillance de la NSA et des spécialistes en sécurité informatique mettent en cause la politique de chiffrement mise en place par Google pour sa nouvelle messagerie.



Haro sur Allo. La nouvelle application de messagerie instantanée de Google était l'une des principales annonces de la conférence Google I/O, mercredi 18 mai, au quartier général de l'entreprise à Mountain View. Fondée sur l'intelligence artificielle, elle est capable de comprendre le langage humain et affine son algorithme au fil des conversations afin de proposer des suggestions de plus en plus pertinentes. Disponible cet été sur Android et iOS, elle est déjà au cœur d'une controverse d'experts. Allo possède des paramètres de sécurité renforcés. Un mode « incognito » permet de chiffrer de bout en bout les messages afin de les rendre illisibles pour une personne extérieure à la conversation. Seuls les participants à la discussion sont en mesure de les déchiffrer. Google lui-même ne peut pas y accéder et répondre à d'éventuelles requêtes judiciaires des autorités. Cette option est basée sur le protocole open source Signal, développé par Open Whispers Systems. C'est le même protocole de chiffrement que WhatsApp, dont les discussions sont cryptées de bout en bout depuis le mois d'avril. Mais à l'inverse de WhatsApp et d'autres messageries sécurisées actuelles (Viber, Signal, iMessage) le chiffrement des conversations n'est pas activé par défaut sur Allo. C'est aux utilisateurs d'effectuer la démarche.

Les experts en sécurité déconseillent Allo

Des experts en cybersécurité s'interrogent déjà sur la pertinence d'une telle fonction, arguant que de nombreux utilisateurs ne feront pas la démarche de l'activer. « La décision de Google de désactiver par défaut le chiffrement de bout en bout dans la nouvelle application de discussion instantanée Allo est dangereuse et la rend risquée. Évitez-la pour l'instant », a conseillé Edward Snowden sur Twitter.

Le lanceur d'alerte à l'origine du scandale des programmes de surveillance de la NSA en 2013 n'est pas le seul à critiquer le choix de Google. Nate Cardozo, représentant de l'EFF, une association américaine de défense des libertés numériques, a estimé pour sa part que « présenter la nouvelle application de Google comme étant sécurisée n'est pas juste. L'absence de sécurité par défaut est l'absence de sécurité tout court ».

« Rendre le chiffrement optionnel est une décision prise par les équipes commerciales et juridiques. Elle permet à Google d'exploiter les conversations et de ne pas agacer les autorités », a encore indiqué Christopher Soghoian, membre de l'Association américaine pour les libertés civiles.

L'intelligence artificielle, priorité de Google

Après avoir pris fait et cause pour Apple dans le bras de fer qui l'a opposé au FBI sur le déblocage de l'iPhone chiffré d'un des terroristes de San Bernardino, Google n'est donc pas allé aussi loin que WhatsApp en généralisant le chiffrement des discussions. Un ingénieur en sécurité de Google a expliqué sur son blog comment la société avait dû arbitrer entre la sécurité des utilisateurs et les services d'intelligence artificielle d'Allo.

Pour profiter pleinement des capacités de Google Assistant implémentées dans Allo, les algorithmes doivent être en mesure d'analyser les conversations, ce qui n'est possible qu'en clair. « Dans le mode normal, une intelligence artificielle lit vos messages et utilise l'apprentissage automatique pour les analyser, comprendre ce que vous voulez faire et vous donner des suggestions opportunes et utiles », explique Thai Duong.

Ce parti pris pourrait évoluer d'ici la sortie de l'application cet été. Le site américain TechCrunch a publié des paragraphes que l'ingénieur avait publié dans son article avant de les supprimer. Il affirme qu'il est en train de « plaider en faveur d'un réglage avec lequel les usagers peuvent choisir de discuter avec des messages en clair », pour interagir avec l'intelligence artificielle en l'invoquant spécifiquement, sans renoncer à la vie privée. En somme, proposer « le meilleur des deux mondes »... [Lire la suite]



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contenus, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Source : *Pourquoi Edward Snowden déconseille Allo, la nouvelle messagerie de Google*