
28/04/2025

Microsoft Recall : séduisant sur le papier, inquiétant en réalité ?

Première réaction à la rédaction : wouah ! Presque immédiatement suivi d'un : « Mais ça veut dire que le PC est monitoré en permanence ? » Car c'est bien de ça qu'il s'agit : une mémoire d'appoint qui, pour fonctionner, capture l'écran toutes les 5 secondes. Alors, Microsoft Recall, vraie ou fausse bonne idée ?

Présenté lors du Surface Event le 20 mai dernier, Microsoft Recall agite les foules. D'un côté, les partisans du progrès et les mémoires courtes, de l'autre, les frileux et les organisés. Et puis, il y a celles et ceux qui, comme nous, s'enthousiasment de voir poindre de nouveaux usages permis par l'évolution technologique, mais ne se cachent pas d'émettre des réserves quant à la manière dont ils sont induits. Et c'est un peu ce qu'il se passe avec Recall : un outil fort ingénieux, mais dont les modalités d'exécution pas toujours claires laissent planer le doute sur la balance bénéfices-risques pour les données personnelles. Recall, celui qui se souvenait de tout quand vous ne vous souveniez pas de grand-chose. Concrètement, il s'agit d'un outil propulsé par l'intelligence artificielle, capable d'historiser tout ce qui a été affiché à l'écran de votre PC (images, texte...) et de retrouver des informations précises que vous auriez oubliées. Un moteur de recherche associé vous permet de saisir une requête en langage naturel (« Retrouve le nom du restaurant coréen dont Alice m'a parlé », pour reprendre l'exemple de Microsoft), et Recall se charge d'analyser l'historique d'affichage pour trouver rapidement la réponse à votre question. Pratique quand on a l'habitude de scroller, survoler, remettre à une date indéterminée... et qu'on est régulièrement sujet aux trous de mémoire. Des détails techniques transparents, mais toujours des zones d'ombre. Ce qu'il faut bien comprendre avec Recall, c'est que s'il peut se constituer mémoire artificielle de l'intelligence humaine, c'est grâce à l'enregistrement permanent de tout ce qu'il se passe à l'écran. Microsoft a donné des détails concernant ce procédé, indiquant que la fonctionnalité sauvegarde des instantanés toutes les 5 secondes, à condition que la nouvelle capture présente un contenu différent de la précédente. Détail qui a son importance : ces instantanés sont stockés localement, chiffrés, au même titre que l'IA derrière Recall qui analyse ces captures localement (OCR locale). En théorie, rien ne devrait s'échapper sur les serveurs de Microsoft. On sait également que l'option n'est pas activée par défaut. Si vous ne l'exécutez pas manuellement une première fois, a priori, il n'y a aucun risque que vous soyez surveillé à votre insu. Vous gardez aussi la main sur un certain nombre de paramètres que vous pouvez modifier à l'envi, comme l'espace de stockage alloué, la suppression des captures sauvegardées, mais aussi les applications et sites web que vous préférez exclure du monitoring, façon split tunneling. À une condition près pour ce dernier cas : il vous faudra utiliser Edge. Concernant la navigation privée, les navigateurs Chromium sont aussi compatibles avec les fonctions d'exclusion. Mais qu'en est-il de toutes les autres informations que vous jugez confidentielles sans pour autant nécessiter d'utiliser la navigation privée ? Vos données administratives personnelles (espaces en ligne, documents téléchargés et ouverts localement, comme votre déclaration de revenus, vos relevés de sécu, vos contrats bancaires), vos numéros de carte bancaire saisis sur une plateforme d'achat en ligne, vos identifiants de connexion peuvent, eux aussi, être immortalisés par Recall toutes les 5 secondes si vous n'avez pas pris soin de désactiver l'option avant et que vous oubliez de supprimer les snapshots dans la foulée. Et si rien n'est officiellement censé transiter sur le Web, nul n'est à l'abri d'un piratage ou d'un simple vol de PC. Nous nous interrogeons aussi sur ce que les

autres peuvent enregistrer de nous à notre insu, au détour d'une conversation, d'un e-mail ou d'une visio. Un peu comme pour les réseaux sociaux qui, grâce aux publications des entourages des uns et des autres, recensent des milliers de photos de personnes qui n'ont jamais demandé à y figurer. Mais alors qu'il est possible de signaler une publication sur Facebook, Instagram et consorts pour la faire retirer, rien ne nous permet, aujourd'hui, d'avoir de contrôle sur les éventuels instantanés Recall de nos interlocuteurs. Et ça, c'est autrement effrayant.

Microsoft Copilot

Intégration de DALL-E 3 pour une création d'images plus créatives et réalistes Capacité de traitement des images par GPT-4 Vision pour des réponses contextuelles précises Interface conviviale et intégrée dans divers produits Microsoft Microsoft Copilot est un chatbot combinant l'intelligence artificielle avancée avec la capacité de générer des images créatives et réalistes grâce à DALL-E 3, et de traiter des requêtes qui reposent sur des images grâce à GPT-4. Cette intégration multimodale en fait un outil polyvalent pour les utilisateurs cherchant à obtenir des informations contextuelles sur des images ou à générer des contenus visuels sur mesure. Microsoft Copilot est un chatbot combinant l'intelligence artificielle avancée avec la capacité de générer des images créatives et réalistes grâce à DALL-E 3, et de traiter des requêtes qui reposent sur des images grâce à GPT-4. Cette intégration multimodale en fait un outil polyvalent pour les utilisateurs cherchant à obtenir des informations contextuelles sur des images ou à générer des contenus visuels sur mesure. clubic

From:
<http://aproposnews.com/> - **Apropos News**

Permanent link:
<http://aproposnews.com/doku.php/elsenews/spot-2024/05/microsoft-recall>

Last update: **23/05/2024**

