Aan:	Tweede Kamer Commissie Digitale Zaken
Van:	Annemarie Costeris, Geff Brown, Scott Bissell, namens Microsoft
Betreft:	Position Paper tbv hoorzittting Microsoft Recall toepassing d.d. 10 september 2024

Hartelijk dank voor uw uitnodiging voor deelname een een hoorzitting over de Recall AI functie van Microsoft, welke op dit moment in de ontwikkelings- en testfase is. Recall beoogt de productiviteit van gebruikers te vergroten door het aanbieden van een nieuwe wijze om eerder bekeken content onmiddellijk te vinden op hun Copilot+ pc's. Recall is nog niet beschikbaar voor het publiek en zal aanvankelijk alleen beschikbaar zijn voor gebruikers die deelnemen aan het Windows Insider Program ("WIP"), per medio oktober. Het aantal WIP-klanten in de EER met een Copilot+ pc is op dit moment ca. 400 personen. Recall zal uitsluitend beschikbaar zijn op Copilot+ pc's; de meest geavanceerde en efficiënte Windows-pc's tot nu toe, die beschikken over verbeterde prestaties en AI-toepassingen. Recall zal in het WIP blijven terwijl Microsoft de kwaliteit van de bouw valideert, feedback van gebruikers meeneemt en de richting en gebruik van het product versterkt.

Deze keuze wordt gemotiveerd door onze inzet voor een veilige en vertrouwde ervaring, terwijl we op zoek zijn naar meer input voordat we functies breed beschikbaar stellen aan gebruikers van Copilot+ pc's. Veiligheid staat voorop bij Microsoft en dit sluit aan bij ons Secure Future Initiative ("SFI"). Wij werken aan het vergroten van de veiligheid van Recall content met maatregelen zoals "just in time" decryptie, beschermd door Windows Hello Enhanced Sign-in Security ("ESS"), die ervoor zorgen dat Recall snapshots alleen worden gedecodeerd na gebruikersverificatie. SFI blijft leidend in de ontwikkeling van Copilot+ PCs, Recall en Windows.

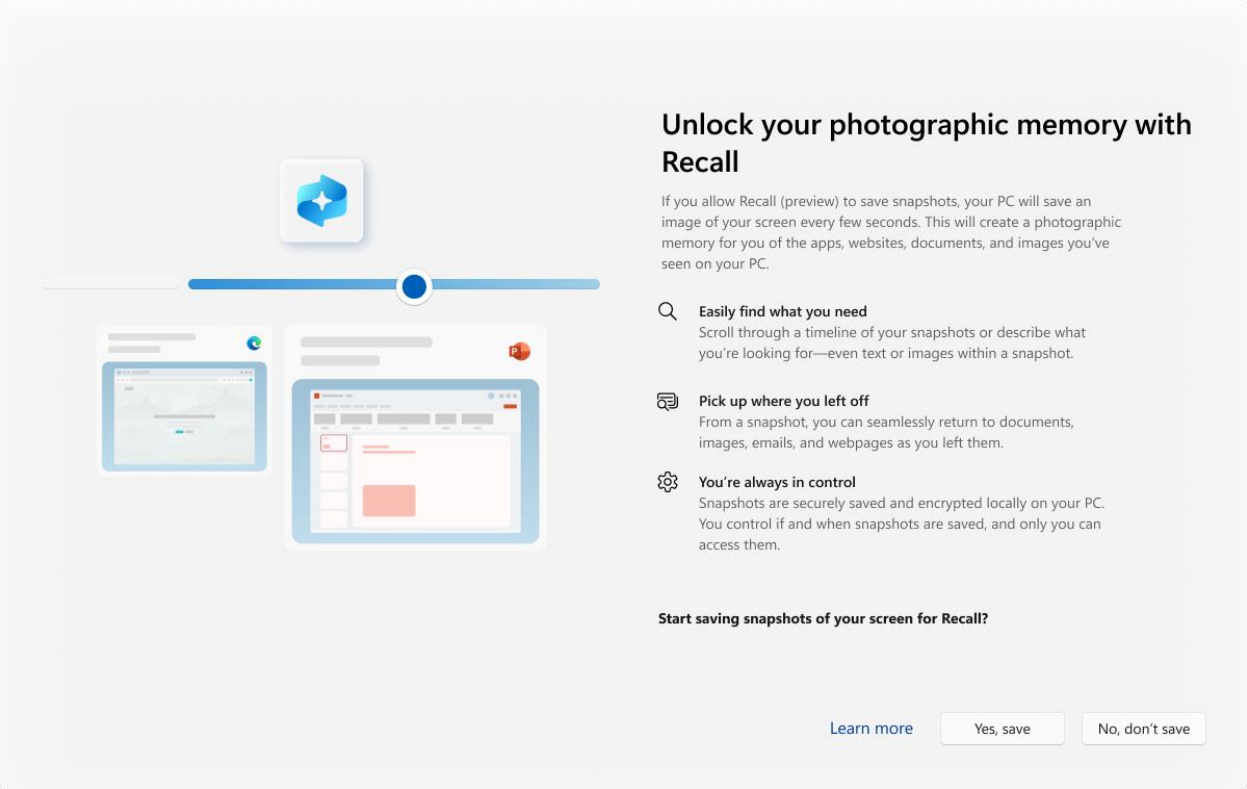
Wat is Recall?

Recall is een functie die gebruikers in staat stelt om snel dingen te vinden die ze eerder hebben gezien of gedaan op hun Copilot+ pc. Recall werkt middels het periodiek nemen van snapshots van wat er op het scherm staat en creëert op die manier een doorzoekbare visuele geschiedenis. Deze snapshots worden lokaal versleuteld, opgeslagen en verwerkt met behulp van de in de pc ingebouwde, lokaal werkende AI om context aan de snapshots mee te geven. Wanneer zij ingelogd zijn kunnen gebruikers via Recall toegang krijgen tot hun persoonlijke visuele zoekgeschiedenis om informatie van eerdere activiteiten te vinden in apps, sites, afbeeldingen en documenten, die functioneren als een privé "fotografisch geheugen". Er wordt in meerdere controlemechanismen voor gebruikers voorzien, met opties om het verzamelen van snapshots te stoppen, tijdelijk op te schorten, apps en websites eruit te filteren die niet als snapshots moeten worden opgeslagen, en om reeds verzamelde snapshots te verwijderen. Bovendien slaat Recall geen content op die beschermd is door het beheer van digitale rechten (*digital right management*, "DRM") en slaat Recall geen content op uit privé-browseractiviteit tijdens het gebruik van Microsoft Edge, Firefox, Opera, Google Chrome, of andere op Chromium gebaseerde browsers.

Microsoft gelooft in het benutten van de revolutionaire mogelijkheden van AI om het leven van mensen te verbeteren. Eén daarvan is het gebruik van de praktische aspecten van Recall om dagelijkse uitdagingen het hoofd te bieden. Net zo belangrijk is het winnen van vertrouwen van de gebruiker in voorzieningen zoals Recall; om die reden bieden wij aanvankelijk uitsluitend toegang via WIP op Copilot+ pc's. Hierdoor kan een subcategorie klanten desgewenst kiezen voor vroeg

gebruik, zodat zij ons waardevolle inzichten kunnen verschaffen over hoe klanten de tool daadwerkelijk gebruiken in werkelijke situaties.

Gebruikers moeten zich aanmelden voor het opslaan van snapshots
Windows vraagt gebruikers om 'opt-in' toestemming te geven voor de Recall functie tijdens de installatie van de Copilot+ pc of bij het toevoegen van Recall aan een bestaande Copilot+ pc. Dit geeft gebruikers de mogelijkheid geïnformeerd te worden over de Recall snapshot-functie en de keuze om snapshots wel of niet op te slaan. Tenzij een gebruiker kiest voor 'opt in', staat de standaardinstelling van deze functie op 'uit'. Hieronder ziet u een voorbeeld van wat een gebruiker te zien krijgt bij de initiële installatie van een Copilot+ pc.



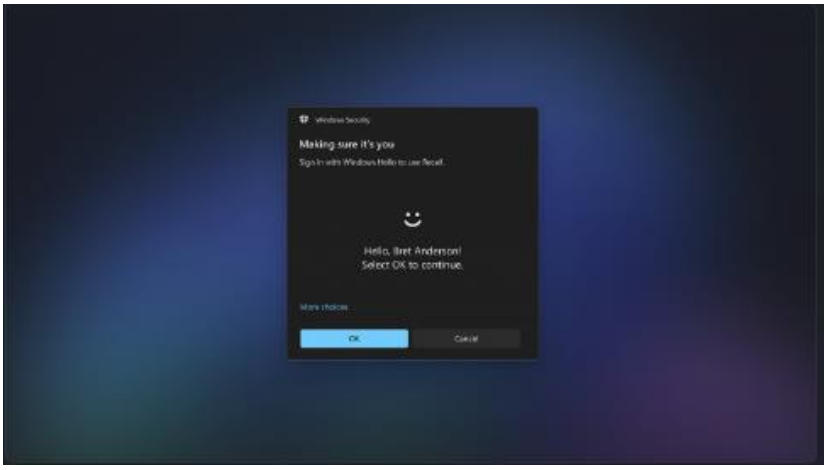
Bij de snapshots horen bepaalde data, waaronder:

(1) Informatie over de app die de gebruiker gebruikt en wat deze op de titelbalk laat zien, waar het wordt opgeslagen, en wanneer de snapshot is genomen.
(2) Screen-understanding, AI-afgeleide data, wat dingen omvat als scherminhoudregio's, beeldregio's, optische tekenherkenning (*Optical Character Recognition*, "OCR") van een tekst, en semantische inbeddingen. Deze data is afkomstig van de analyse van de snapshots door de AI.
(3) Door de app geleverde data over activiteit - bevat een link die de applicatie opnieuw kan opstarten naar een specifieke view of pagina.

Om Recall te laten werken met schermcontent, zoals tekst of afbeeldingen, ondergaan foto's lokale bewerking met *Optical Character Recognition* ("OCR"). Dit helpt om inzicht te krijgen in de content die op het scherm stond, zoals tekst en beeld content (bijv. een pizza, hond of bal). Dit wordt gebruikt om relevante resultaten te identificeren wanneer de gebruiker een zoekopdracht geeft binnen Recall. Deze technologie isoleert interessegebieden in de screenshots, bijvoorbeeld door onderscheid te maken tussen blokken tekst en afbeeldingen. Het past ook OCR toe om een tekst te transcriberen en genereert semantische inbeddingen voor zowel tekst als afbeeldingen om latere zoekopdrachten via Recall te verbeteren. Zowel snapshots als hun bijbehorende data, plus de semantische index, worden lokaal bewaard op het de pc.

Veilig door ontwerp en veilig als standaard

Om Recall te openen en toegang te krijgen tot de tijdlijn en zoekopdracht moeten gebruikers zich aanmelden via Windows Hello verificatie. Microsoft verbetert de databeveiliging voor de aanstaande "preview"- lancering van Recall door het invoeren van just-in-time decodering van Recall data met Windows Hello ESS. Dit betekent dat snapshots uitsluitend na verificatie gedecodeerd en toegankelijk gemaakt worden. Bovendien zijn de bijbehorende data en zoekindex-database versleuteld, om de bescherming van Recall te versterken naast eerder bestaande Windows Security features, zoals SmartScreen en Defender, die gebruik maken van AI om malware te blokkeren.



Eén van de meer effectieve manieren om gegevens op een pc te beschermen is door de pc zélf te beveiligen. Copilot+ pc's zijn zo toegerust dat ze vanaf de start veilig zijn, bijvoorbeeld door verbeterde firmware verdediging en Windows Hello Enhanced Sign-in beveiliging, die veilige biometrische toegang mogelijk maakt.

Beschermen van gebruikersprivacy op Copilot+ pc's

Recall is toegerust met verschillende instellingen waarmee gebruikers hun ervaring kunnen aanpassen naar hun privacyvoorkeuren, wat helpt bij het waarborgen van hun gegevensbescherming en individuele autonomie ten aanzien van hun voorkeuren voor het vastleggen van snapshots (voor meer informatie, zie dit blog). Onder andere gaat het om:

- Snapshots worden alleen op het lokale apparaat opgeslagen. Copilot+ pc's zijn uitgerust met geavanceerde AI die uitsluitend werkt op de pc, zonder dat er internet- of cloud-gebaseerde

interacties nodig zijn om snapshots op te slaan of te verwerken. Alle AI-verwerking voor Recall wordt op het apparaat zelf uitgevoerd, waarbij snapshots veilig en privé worden gehouden op de pc. De AI op Copilot+ pc's gebruikt deze snapshots niet om de AI op Copilot+ pc's te trainen.

- Snapshots blijven privé. Recall geeft geen snapshots door aan Microsoft. Snapshots worden vertrouwelijk behandeld en worden niet gedeeld met andere applicaties of organisaties. Bovendien deelt Recall geen snapshots tussen gebruikers op hetzelfde apparaat, en versleuteling op individueel niveau zorgt ervoor dat zelfs beheerders geen toegang hebben tot snapshots van andere gebruikers.
- Gebruikers zullen meldingen ontvangen van snapshot activiteit. Wanneer Recall actief is verschijnt dit op de taakbalk zodra er toegang is tot de desktop. Er is ook een icoontje in het systeemvak dat aangeeft wanneer Windows snapshots actief vastlegt.
- Bepaalde content is uitgesloten van snapshots. Recall is zo geprogrammeerd dat het snapshots niet opslaat tijdens het bekijken van door digitale rechten beheerde content of tijdens InPrivate browsingsessies in Microsoft Edge, Firefox, Opera, Google Chrome, of ander Chromium-gebaseerd browser aanbod.
- Gebruikers hebben het volledige beheer over snapshots. Het is aan de gebruiker wat wordt opgeslagen in een snapshot. Gebruikers zullen het opslaan van snaphots afwisselend aan- en uit kunnen zetten via Instellingen > Privacy & beveiliging > Recall & snapshots. Gebruikers zullen het vastleggen van snapshots tijdelijk kunnen pauzeren door te klikken op het Recall-icoontje in het systeemvak en de pauze-optie te kiezen. Recall-instellingen geven gebruikers de mogelijkheid om bepaalde applicaties en websites in ondersteunde browsers (Microsoft Edge, Firefox, Opera en Google Chrome) uit te sluiten van snapshots. Bovendien kunnen snapshots altijd worden verwijderd als de gebruiker daarvoor kiest.
- In gevallen waarin apparaten beheerd worden door een IT-afdeling zal de beheerder het opslaan van snapshots kunnen uitschakelen door middel van beleid voor groepsbeheer of mobiele apparaten-beheer. Beheerders hebben echter geen toestemming om het opslaan van snapshots voor de eindgebruiker te *activeren*; dit is een besluit dat aan de individuele gebruiker alleen voorbehouden blijft. Als op een later moment een beleid wordt ingevoerd om het opslaan van snapshots uit te zetten, zullen alle voorheen opgeslagen snapshots worden gewist en zullen gebruikers op die apparaten de feature 'opslaan van snapshots' niet kunnen heractiveren.

Microsoft blijft openstaan voor feedback en blijft zoeken naar mogelijke verbeteringen aan de producten en diensten die wij aanbieden.

Mensen 'empoweren' met ervaringen die zij kunnen vertrouwen

Het is Microsoft's missie om producten te maken die mensen en organisaties in staat stellen om meer te bereiken, waarbij Microsoft sterk inzet op het beschermen van de privacy, de veiligheid en het vertrouwen van klanten. Wij zullen klant-feedback blijven gebruiken van consumenten, ontwikkelaars en bedrijven om ons aanbod te verfijnen op een wijze die relevant is voor die doelgroepen.

De introductie van Copilot+ pc's en Recall markeert een volgende stap vooruit naar innovatieve features en voordelen in deze nieuwe categorie pc's. Onze focus op het ontwikkelen van deze mogelijkheden zet privacy, veiligheid en beveiliging voorop.