New Windows 11 Feature Causing Privacy Concerns

May 26, 2024 - At the recent Build conference, Microsoft introduced an innovative AI-powered feature for Windows 11 named "Recall." This feature, aimed at Copilot+ PCs, is designed to capture and store snapshots of a user's screen activity every few seconds. While it promises to significantly enhance user experience by providing a detailed log of past activities, it also raises serious privacy concerns, particularly if a PC is lost or stolen.

Recall utilizes the advanced processing capabilities of Copilot+ PCs to continuously document what a user does on their computer. This includes capturing activities in applications, communications during live meetings, and websites visited. These snapshots are encrypted and stored locally, enabling users to search and navigate through their activity history via a timeline feature.

Currently, only a minority of computers in use are capable of utilizing Recall. Thatâ€™s because users must have one of the new Copilot Plus PCs equipped with Qualcommâ€™s Snapdragon X Elite chips, which are necessary for the feature's neural processing capabilities. PCs with the minimum capabilities required for recall will store approximately three months of snapshots, though users can adjust the storage allocation according to their preferences. The service is currently in a preview phase, during which Microsoft is gathering user feedback and refining the feature, particularly for enterprise customers. A broader release will follow once these enhancements are complete.

Despite Microsoft's assurances about encryption and that all snapshots will be held on local storage, the privacy implications of Recall are substantial. If a PC is lost or stolen, anyone who gains access to the userâ€™s account could potentially view an exhaustive record of their digital activities. This risk is especially concerning for journalists, activists, and other individuals who may be targeted for their work or viewpoints.

The extensive data captured by Recall could also be used by government agencies or private investigators, raising concerns about surveillance and evidence collection. The detailed nature of the information â€“ including personal communications and browsing histories â€“ necessitates a careful consideration of the trade-offs between convenience and privacy.

To address these concerns, Microsoft has implemented several features. Users can pause, stop, or delete captured content and exclude certain apps or websites from being recorded. Recall also does not capture snapshots during InPrivate browsing sessions in Microsoft Edge or of DRM-protected content. While these features may be beneficial to users with some technical background, history shows that most people only have a vague idea about how to manipulate their computerâ€™s operating system. IF computers are shipped with Recall turned on, we suspect that the vast majority of users wonâ€™t have any idea how to change its settings or turn it off.

Making matters worse, Recall does not automatically mask sensitive information such as passwords or financial details, which could still be visible in the snapshots. This has the potential to expose this information to anyone who can gain access to a Recall enabled computer.

Microsoftâ€™s position appears to be that Recall represents a significant advancement in how AI can enhance the user experience on Windows 11. But the risks associated with Recall may very well outweigh any benefits. Our suggestion to anyone purchasing a computer with this capability is to educate yourself first, or turn it off entirely.
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS