New Outlook and Recall: A Privacy Nightmare

Kieren Niĉolas Lovell

June 7, 2024

Kieren Niĉolas

Abstract

This article discusses the privacy concerns and data collection practices associated with the new Microsoft Outlook for Windows, introduced in the latest Windows 11 update. By default, this updated Outlook syncs user data, including credentials and emails, to Microsoft Cloud, even for third-party accounts like Gmail, unless users opt out. The reports highlight significant privacy issues and the extensive data collection facilitated by this feature. Additionally, the introduction of Microsoft Recall, which continuously takes "screenshots" of the user's PC to create a searchable database, raises further concerns about user privacy and data security.

Keywords: *Information Security, Outlook, New Outlook*

E-mail address: kieren@kierennicolas.com
Revised: June 7, 2024

1. Introduction

The recent updates in Windows 11 introduce significant changes to Microsoft's approach to user privacy. The new Microsoft Outlook, replacing the existing Calendar and Mail applications, and the newly introduced Copilot+ Recall feature, which continuously takes screenshots of the user's PC, have raised substantial privacy concerns.

2. New Outlook: Data Collection Practices

The updated Microsoft Outlook for Windows, by default, syncs user data, including credentials and emails, to Microsoft Cloud, even for third-party accounts like Gmail, unless users opt out. This practice has highlighted several key privacy concerns.

According to Microsoft's privacy policy, 772 third parties currently have access to user data through Outlook. This extensive data collection is suggested to serve primarily for advertising purposes. Key points of concern include:

- **Extensive Data Collection**: The New Outlook app gathers a wide range of user data, including emails, contacts, events, geolocation data, and browsing history.
- **Opt-out, Not Opt-in**: Users are required to manually opt out of data sharing with each third party, rather than having the option to opt-in from the start. This makes protecting privacy difficult and time-consuming.
- **Lack of Transparency**: Microsoft has been criticised for its lack of clarity regarding the collection and storage of user data. The privacy policy is complex, and it is not always clear how the data is used [6].

Despite Microsoft's assurance that users can switch back to previous apps at any time, the company will already store the data, effectively allowing Microsoft to read users' emails.

3. Details of the New Outlook

In a report by heise.de, it was found that New Outlook users risk having their IMAP and SMTP credentials and entire emails transferred to Microsoft servers without proper consent (see figure 1). When users want to add their email accounts from different providers, such as Gmail, a pop-up informs: "For a better experience, your messages, events, and contacts will be synced to the Microsoft Cloud." This means that Microsoft will store duplicate copies on its servers [5].

Adding an account to Outlook involves synchronising it with the Microsoft Cloud, as stated on the Microsoft support page: "Syncing your account to the Microsoft Cloud means that a copy of your email, calendar, and contacts will be synchronised between your email provider and the Microsoft data centres." The New Outlook app is now recommended over the Mail app and is available with the "New Outlook" switch for Microsoft 365 subscribers.

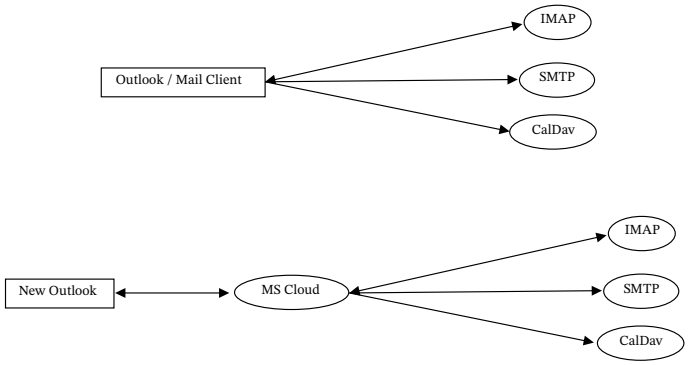

Figure 1. Outlook and New Outlook Mail Transfer Flow

4. Security Concerns

Heise.de raised concerns about the data that Microsoft is transmitting and storing. The publication observed that Microsoft was creating copies of the user credentials, including usernames, passwords, and server information, and transmitting these datapoints in plain text, despite using Transport Layer Security (TLS) for encryption. Heise.de warns: 'Without informing or asking, Microsoft grants itself full access to the IMAP and SMTP access data of users of the New Outlook" [5].

Microsoft claims that this is to "enhance your Microsoft 365 experience in New Outlook for Windows," enabling the synchronisation of non-Microsoft accounts, including Gmail, Yahoo, iCloud, and IMAP accounts, across Outlook for iOS, Android, and Mac. A Microsoft spokesperson explained that, "Syncing a user's IMAP account helps the user have a consistent experience for all accounts added in Outlook, such as being able to use mail search and mark emails as read/unread. For IMAP providers that use BasicAuth, we store access data as an encrypted user token in the user's own mailbox. For providers that support OAuth (Gmail and Yahoo Mail), Microsoft does not have access to user access data in plain text" [3].

Despite these assurances, cybersecurity communities are concerned. One user on Hacker News speculated, "They're going to use your email for training AI models, trying to catch up with Google in every way possible, disregarding user trust, privacy, and security" [4].

5. Recall: Additional Privacy Issues

Adding to the privacy concerns is the Copilot+ Recall feature in Windows 11, which continuously takes "screenshots" of the user's PC, creating an instantly searchable database of everything the user has ever seen on their screen. Although Microsoft CEO Satya Nadella

describes it as a "photographic memory" of the PC, the feature has raised significant privacy concerns among users and cybersecurity experts [1].

CyberCX's Digital Forensics and Incident Response (DFIR) team has also evaluated Recall for its forensic value. Despite the privacy concerns, Recall can be beneficial for forensic investigations [2]. The team set up Recall on an Azure VM with ARM64 CPUs, using tools like AmperageKit to enable the feature, and performed various tests to assess its capabilities.

5.1. Forensic Applications of Recall

Recall utilises the Windows Copilot Runtime to periodically take screenshots and store them locally. The stored data includes processed Optical Character Recognition (OCR) text, which makes searching for activities much faster. The main artefacts identified during testing include:

- **Evidence of Execution**: Commands typed into a terminal and app execution are recorded.
- **Evidence of File Folder Interaction**: Interaction with files and folders is captured.
- **Evidence of Presence/Existence**: Existence of files, folders, and apps is documented.
- **Timestamps of Activity**: Detailed timestamps of various activities are recorded.

These artefacts are stored in the 'ukg.db' SQLite database and the 'ImageStore' folder, which contains JPEG images of each snapshot. The 'WindowCapture' table within the database logs when windows are created, changed, and when a snapshot is taken. This table can be enriched with data from the 'App' table to link windows to specific processes.

5.2. Artefact Summary

The 'ukg.db' database includes several tables:

- **App & AppDwellTime Tables**: Information on processes that create windows and tracking of how long the window has been open.
- **WindowCapture Table**: Logs window creation, changes, and snapshots, including window titles and IDs.
- **WindowCaptureAppRelation Table**: Links window captures to specific processes.
- **WindowCaptureTextIndex_content Table**: Stores OCR text from window snapshots.

For example, running commands in the Windows Terminal app records not only the commands but also the outputs, providing a detailed log of activities. However, the feature does not capture content in incognito mode or applications that use 'SetWindowDisplayAffinity' functionality.

The reaction to Copilot+ Recall has been overwhelmingly negative. Although it may benefit managers who need to quickly search for past activities, for most users, the idea of their entire PC activity being recorded and searchable is alarming. Critics argue that it undermines the personal nature of Windows and poses significant privacy risks.

Beaumont explains that every few seconds, the Azure AI takes and processes the screenshots, stored in an SQLite database in the user folder. This database contains a record of everything that is viewed on the PC in plain text. Despite Microsoft's assurances that data are processed locally and encrypted, Beaumont demonstrates that hackers can access these data remotely, making them vulnerable to InfoStealer trojans and other malware [1].

The Copilot+ Recall feature not only stores all websites visited and all viewed text, but also keeps deleted emails and messages, making them available indefinitely. Beaumont warns that this could lead to mass data breaches, with hackers able to easily extract detailed user data [1].

6. Conclusion

The recent changes in Microsoft's approach to user privacy through the New Outlook and Copilot+ Recall features necessitate a thorough re-evaluation. While ProtonMail, a direct competitor of Microsoft, has underscored these issues, the concerns raised and the data cited merit further examination and reflection. Microsoft has not yet provided a comprehensive public response to these specific concerns, leaving numerous users uncertain about the full ramifications of these features.

To ensure alignment with stringent security and privacy standards, Microsoft must fundamentally reassess and redevelop both the New Outlook and Recall features. The potential failure to address these critical issues could profoundly undermine user trust in Microsoft's Copilot and its broader security offerings [1].

References

[1] K. Beaumont, "Copilot+ recall: How microsoft's new feature compromises user privacy," *DoublePulsar*, Jan. 2024. [Online]. Available: https://doublepulsar.com/copilot-recall-privacy-issues-6008506.

[2] L. Davis, "Forensic Applications of Microsoft Recall," *CyberCX*, Jun. 2024. [Online]. Available: https://cybercx.com.au/blog/forensic-applications-of-microsoft-recall.

[3] Microsoft, *New outlook for windows*, Jan. 2024. [Online]. Available: https://support.microsoft.com/en-us/new-outlook-for-windows.

[4] H. News, "Discussion on microsoft's new outlook data sync practices," *Hacker News*, Jan. 2024. [Online]. Available: https://news.ycombinator.com/item?id=30000000.

[5] H. Online, "Microsoft's new outlook syncs user data to its cloud by default," *Heise Online*, Jan. 2024. [Online]. Available: https://www.heise.de/newsticker/meldung/Microsoft-s-New-Outlook-syncs-user-data-to-its-cloud-by-default-6008346.html.

[6] ProtonMail, "Microsoft's new outlook for windows app: The privacy nightmare nobody asked for," *ProtonMail Blog*, Jan. 2024. [Online]. Available: https://protonmail.com/blog/new-outlook-privacy-concerns.