Signal restricts OS-level AI assistants from reading private conversations



Signal now blocks screen capture by AI assistants such as Siri AI on iOS 27 and Gemini on Android. The protections have gaps, notably on macOS and for on-device files, so institutions should review their own exposure.

- Signal blocks in-app screenshots on iOS 27 to stop Siri AI reading message content, controlled by a Block Siri AI setting.
- On Android the app detects AI assistants trying to read the screen and enables Screen security automatically.
- Limits remain: an agent could still reach content stored on the device, and macOS lacks equivalent protection.
- macOS 27 users are advised to add Signal to the Excluded Apps list under System Settings > Siri.

> - Signal asks Apple, Google and Microsoft for a documented opt-out from AI access to screen content, files, notifications and APIs.

Signal has introduced protections that stop AI assistants built into mobile operating systems from capturing the content of conversations. They cover Siri AI on iOS 27 and assistants on supported Android devices, including Google's Gemini.

Why it matters

These assistants can read what is on the phone's screen to answer questions and perform tasks. Signal explains that this can copy message text into a local database or a remote server operated for the assistant, placing it outside the app's control and exposing every participant in the conversation, not only the device owner.

How the protections work

On iOS 27, Signal blocks screenshots inside the app so Siri AI cannot read messages through the screen; a Block Siri AI setting governs this. On Android, the app detects an assistant attempting to read the screen and turns on its Screen security setting automatically, because many vendors offer no reliable way to detect screenshot attempts.

Signal is open about the limits. An AI agent could still retrieve content stored on the device through the filesystem. On macOS, Signal cannot reliably block screenshots, so it recommends that macOS 27 users add Signal to the Excluded Apps list under System Settings > Siri. Users can switch the protection off, but doing so may expose their messages and their contacts' messages to assistants.

Signal is asking Apple, Google and Microsoft for a documented way for apps to opt out of AI access to screen content, files, notifications and APIs, along with clearer documentation of how agents handle data.

What to do next

For regulated institutions, the practical point is that OS-level assistants can reach sensitive on-screen content in any app. The steps below help bring this into existing mobile and data-protection controls.

What to do now

1. Inventory which staff use Signal or similar messaging apps for work and which OS-level AI assistants are enabled on those devices.
2. Update mobile device management and acceptable-use policies to cover AI assistants with screen-reading access.
3. Advise staff to keep Signal's Block Siri AI and Screen security settings enabled, and to add Signal to Excluded Apps on macOS 27.

4. Assess whether classified or personal data discussed in messaging apps could reach assistant databases, and reflect this in PDPL and NCA ECC risk assessments.
5. Raise the documentation gap with your device and OS vendors and request clear details on how assistants process app data.