Signal adds protections to stop AI assistants capturing chats on iOS and Android



Signal has announced protections that block screenshots on iOS 27 and stop AI assistants from capturing conversations on supported Android devices. The source excerpt gives few further details.

- Signal announced new protections against capture of chat content by AI assistants.
- On iOS 27, the protection blocks screenshots.
- On supported Android devices, it prevents AI assistants from capturing conversations.
- The headline names Siri and Gemini as the assistants of concern.
- The available source text does not describe rollout timing or configuration options.

What was announced

Signal has announced new protections aimed at keeping conversations out of reach of on-device AI assistants. On iOS 27 the app will block screenshots, and on supported Android devices it will prevent AI assistants from capturing chat content. The source headline names Siri and Gemini as the assistants in question.

What the source does not say

The excerpt available to us does not explain how the protections work, when they will be released, which Android devices count as supported, or whether users must switch them on. We have therefore not assumed any of these details, and readers should confirm them against Signal's own release notes before relying on the feature.

Why it matters for regulated institutions

AI assistants built into phones can read what appears on screen, which creates a possible route for sensitive business conversations to reach assistant services. Institutions whose staff use Signal for work discussions may wish to understand this exposure, and to review how mobile device policy treats AI assistant features generally, whatever messaging app is used.

The announcement is a product-level control and does not replace organisational measures. Approved communication channels, data classification rules and device management remain the primary safeguards for confidential information.

What to do now

1. Check Signal's official release notes for availability, supported Android devices and any required settings.
2. Review mobile device policy for how OS-level AI assistants may access on-screen content.
3. Confirm which messaging apps are approved for business use and what may be discussed on them.
4. Brief staff who handle sensitive information on the risk of AI assistants reading screens.