Screen-Reading AI Defense & Privacy Audit

Step-by-step checklist to audit what AI can see on your phone or PC screen and how to turn off automatic capture.

Security Context (November 2026): Signal began restricting screenshots on Android and iOS after calling operating systems with screen-reading AI an *existential threat* to personal privacy. If an OS captures your screen to feed an AI agent, your encrypted chats are compromised before leaving the phone.

ANDROID 1. Turn Off Screen-Reading on Android

- [ ] **Disable Circle to Search context:** Settings > Display > Navigation mode > Toggle off *Use screen context* so Google does not scan visible text or images.
- [ ] **Audit Gemini / Google Assistant screen access:** Google app > Settings > Google Assistant > General > Turn off *Use screen context* across all apps.
- [ ] **Pixel Screenshots (Pixel 9+ users):** Settings > Apps > Pixel Screenshots > Turn off background automatic scanning of sensitive receipts and chats.
- [ ] **Enable Signal Screen Security:** In Signal > Settings > Privacy > Advanced > Turn on *Screen security* (blocks screenshots and app switcher previews).

IOS / IPHONE 2. Tame Siri & Apple Intelligence

- [ ] **Restrict Siri on-screen context:** Settings > Siri > When interacting with Siri > Turn off *Show on-screen context* for private messaging and banking apps.
- [ ] **Isolate private apps from Suggestions:** Settings > Privacy & Security > Turn off predictive learning for WhatsApp, Signal, and finance apps.
- [ ] **Signal iOS screen privacy:** Signal > Settings > Privacy > App Switcher > Turn on *Hide screen in app switcher* to avoid background system snapshots.

WINDOWS 11 3. Restrict Windows Recall & Copilot

- [ ] **Audit Windows Recall (Copilot+ PCs):** Settings > Privacy & security > Recall & snapshots > Turn off *Save snapshots* entirely or exclude your browsers and password manager.
- [ ] **Copilot Local File Actions:** When Copilot asks to organize Downloads: choose *"Allow for this session"* or *"Not now"*; never grant indefinite full-disk access.
- [ ] **Copilot in Edge:** Edge Settings > Sidebar > Copilot > Turn off *Allow Microsoft to access page content*.

ALERT 4. Browser Agents (Meta Muse & Injections)

- [ ] **Log out of sensitive accounts:** If running agentic browser extensions (like Muse in Chrome) that click and fill forms, run them in a separate browser profile without logged-in banks.
- [ ] **Prompt injection defense:** Security researchers proved hidden text on third-party web pages can hijack agents and leak memories. Always keep click-by-click manual approvals enabled.

Tested human takeaway: Your chat privacy does not just depend on end-to-end encryption; it depends on whether the operating system displaying the screen is feeding an AI.

✓ TESTED BY HUMANS

Disclaimer: This document is intended solely for general guidance and informational purposes; it does not constitute legal, financial, or formal professional advice.