Android System SafetyCore

Article status notice: This article has been marked as incomplete

This article needs additional work for its sourcing and verifiability to meet the wiki's Content Guidelines and be in line with our Mission Statement for comprehensive coverage of consumer protection issues. In particular:

1. The incident is based mostly on speculation and (warranted) suspiciousness with Google's actions. More sources are needed or change of scope/deletion of the incident.
2. This is currently formatted as a product page, it may be a candidate to turn into an incident

This notice will be removed once the issue/s highlighted above have been addressed and sufficient documentation has been added to establish the systemic nature of these issues. Once you believe the article is ready to have its notice removed, please visit the Moderator's noticeboard, or the discord and post to the `#appeals` channel.

Learn more ▼

Android System SafetyCore is an app developed and released by Google for the Android platform. According to Google the software provides locally-run nudity censoring for any Android devices running version 9 (pie) or later.[1]

Consumer impact summary [edit | edit source]

User Freedom: Can be uninstalled, however a lack of communication and difficulty to find the installed app should call this freedom into question.

User Privacy: Claimed to "only scan files sent on messages app"[1]

Incidents [edit | edit source]

This is a list of all consumer protection incidents related to this product. Any incidents not mentioned here can be found in the .

Android System SafetyCore

Basic Information

Release Year	2025
Product Type	Software
In Production	Yes
Official Website	N/A

Installation without informed consent (January 22, 2025) [edit | edit source]

In January 22, 2025, Google quietly rolled out Android System SafetyCore to all Android devices. The installation of the program neither informed consumers that it was installed, nor did it request consumers to install it onto their devices.[2][3] This additionally bypassed any features consumers have enabled that blocks installations of programs without consumer approval first.

Due to a lack of both transparency or open sourcing, it has brought significant amounts of concern from consumers, especially those who work in tech security. [4][5][6][7] With Google directly stating that the program scans photos that are sent on the messages app, it has set a precedent for this concern as well, since malicious actors or Google themselves could theoretically hijack this product for illicit purposes, such as setting the app to scan for more than just mature photos, or scanning files beyond just what the messages app is allowed.

This lack of transparency has been also cited as a concern from GrapheneOS maintainers, stating that because it is not open source, they will not be including the app inside their operating system.[8]

See also [edit | edit source]

- Android
- Google

References [edit | edit source]

1. ↑ 1.0 1.1 "5 new protections on Google Messages to help keep you safe". *Google Security Blog*. 22 Oct 2024. Retrieved 15 Apr 2025.
2. ↑ Thitu, Naftary (10 Feb 2025). "Rogue or Safe App? Unmasking Android System SafetyCore". *techweez*. Retrieved 15 Apr 2025.
3. ↑ "Android System SafetyCore". *Reddit*. Retrieved 15 Apr 2025.
4. ↑ "Android System SafetyCore: Hidden Installation and What You Should Know". *ProtectStar*. 11 Feb 2025. Retrieved 15 Apr 2025.
5. ↑ "Guys help some app called android system safetycore installed automatically". *Reddit*. Retrieved 15 Apr 2025.
6. ↑ @dancytron (8 Feb 2025). "Android System SafetyCore". *Puppy Linux Discussion Forum*. Retrieved 15 Apr 2025.
7. ↑ @Phosphate5 (12 Feb 2025). "Android System SafetyCore is being silently installed on android devices". *Artix Linux Forum*. Retrieved 15 Apr 2025.
8. ↑ @GrapheneOS (8 Feb 2025). "The functionality provided by Google's new Android System SafetyCore app available through the Play Store is covered here: https://security.googleblog.com/2024/10/5-new-protections-on-google-messages.html Neither this app or the Google Messages app using it are part of GrapheneOS and neither will be, but GrapheneOS users can choose to install and use both. Google Messages still works without the new app. The app doesn't provide client-side scanning used to report things to Google or anyone else. It provides on-device machine learning models usable by applications to classify content as being spam, scams, malware, etc. This allows apps to check content locally without sharing it with a service and mark it with warnings for users. It's unfortunate that it's not open source and released as part of the Android Open Source Project and the models also aren't open let alone open source. It won't be available to GrapheneOS users unless they go out of the way to install it. We'd have no problem with having local neural network features for users, but they'd have to be open source. We wouldn't want anything saving state by default. It'd have to be open source to be included as a feature in GrapheneOS though, and none of it has been so it's not included. Google Messages uses this new app to classify messages as spam, malware, nudity, etc. Nudity detection is an optional feature which blurs media detected as having nudity and makes accessing it require going through a dialog. Apps have been able to ship local AI models to do classification forever. Most apps do it remotely by sharing content with their servers. Many apps have already have client or server side detection of spam, malware, scams, nudity, etc. Classifying things like this is not the same as trying to detect illegal content and reporting it to a service. That would greatly violate

people's privacy in multiple ways and false positives would still exist. It's not what this is and it's not usable for it. GrapheneOS has all the standard hardware acceleration support for neural networks but we don't have anything using it. All of the features they've used it for in the Pixel OS are in closed source Google apps. A lot is Pixel exclusive. The features work if people install the apps" . *X*. Retrieved 15 Apr 2025. `{{cite web}}`: External link in `|title=` (help)

Categories: CS1 maint: numeric names: authors list | CS1 errors: external links | Articles in need of additional work | Articles with verification concerns or other deficiencies | Android

This page was last edited on 15 April 2025, at 20:52.