NetMonster privacy policy

Michal Mroček

Updated: Sunday 12th February, 2017

To make application work properly several potentially dangerous Android permissions are required.

1 Personal information

No personal information is collected.

2 Nonpersonal information

2.1 Phone state

This permission is not mandatory to run NetMonster properly and is not required to be granted after first run. NetMonster requires Android permission called android.permission.READ_PHONE_STATE. This permission is used to access following information:

- since Android 7.0 - data and voice network type (GPRS, EDGE, UTMS, HSPA+, LTE, ...),
- since Android 6.0 - VoWiFi, VoLTE availability, preferred CS Fallback network type, preferred VoWiFi usage
- since Android 5.1 - dual SIM availability.

Information provided by mentioned permission is processed and displayed on screen called "Live". All of gained information is not stored in device’s database nor transmitted to other databases or places on the planet Earth. It is just cached in local random access memory for a few seconds (eventually minutes, depending on Java’s garbage collector).

2.2 Location

NetMonster also needs location permission. Without it system Android does not provide all information connected with network cells that your phone is currently using. List of cells your device was connected to is stored only in local database. NetMonster does not save or track your precise location.

3 Changes to the privacy policy

Right to change this policy at any time is being reserved. Changes to this privacy policy are effective as of the stated "Updated" and your continued use of the app on or after the "Updated" date will constitute acceptance of, and agreement to be bound by, those changes.