1. Compare and contrast various types of security controls

Security control

It offers a range of measures to mitigate risks, detect incidents, and ensure compliance with current regulations.

Control Categories

The four main control categories are

1. Technical
2. Managerial
3. Operational
4. Physical

Technical Controls

- It minimizes vulnerabilities within an organization's technical systems, including computer networks, software, and data management.
- Their primary focus is on upholding system integrity, mitigating the risk of unauthorized access, and protecting sensitive data from potential threats.
- Examples of technical controls are as follows:

  Firewalls:
  - These are a common technical control used to protect computer networks from unauthorized access.
  - They monitor incoming and outgoing network traffic, filter and block potential threats, and reduce the risk of unauthorized intrusion.

  Data encryption:
  - It is a technical control that converts sensitive information into a coded form, making it unreadable to unauthorized individuals.
  - It reduces the risk of data breaches by ensuring that even if data is intercepted, it remains secure and inaccessible without the decryption key.

Managerial Controls

- They encompass the implementation of policies, procedures, and practices by management to guide and direct the activities of individuals and teams.
- By providing clear guidance and oversight, managerial controls contribute to a proactive approach to risk reduction and help safeguard the organization's success.
- Examples of managerial controls include the following:

  Performance reviews:
  - These are a managerial control that involves regular assessments of employee performance.
  - By providing feedback, setting goals, and identifying areas for improvement, performance reviews help align employee activities with organizational objectives and ensure that employees are performing effectively.

Risk assessments:

- These are a managerial control that involves the systematic identification, evaluation, and mitigation of potential risks within an organization.
- By conducting regular risk assessments, management can proactively identify and address potential threats, reducing the organization's overall risk exposure.

Code of conduct:

- A code of conduct is a set of guidelines and ethical standards established by management to govern employee behaviour.
- It serves as a managerial control by defining acceptable behaviour, promoting ethical conduct, and reducing the risk of misconduct within the organization.

Operational Controls:

- These revolve around the execution of day-today activities and processes necessary for delivering goods and services.
- They involve managing operational procedures, ensuring adherence to quality standards, enhancing productivity, and optimizing efficiency.
- These can enhance their overall performance and achieve their objectives effectively.
- Examples of operational controls are as follows:

Incident response procedures:

- These are operational controls that outline the steps to be followed in the event of a security incident or breach.
- These procedures provide a structured approach to detecting, responding to, and recovering from security incidents.
- By having well-defined incident response procedures in place, organizations can minimize the impact of security breaches, mitigate further risks, and restore normal operations more effectively.

Security awareness training:

- It is an operational control that educates employees about security threats, best practices, and organizational policies.
- By providing regular training sessions and updates, organizations reduce the risk of security incidents caused by human error or negligence and create a proactive defence against cyber threats.

User access management:

- It is an operational control that involves the management and control of user access privileges to systems, applications, and data.
- It includes processes for user provisioning, access requests, access revocation, and periodic access reviews.
- By implementing strong user access management controls, organizations can reduce the risk of unauthorized access, protect sensitive information, and ensure

that users have appropriate access privileges aligned with their roles and responsibilities.

Physical Controls

- These are a crucial aspect of overall security, focusing on the protection of an organization's tangible assets, facilities, and resources.
- These aim at preventing unauthorized access, ensuring safety, and mitigating physical security risks.
- By controlling who has access to sensitive or restricted areas, organizations can minimize the risk of unauthorized individuals compromising security or gaining access to critical assets.
- The following are examples of physical controls:

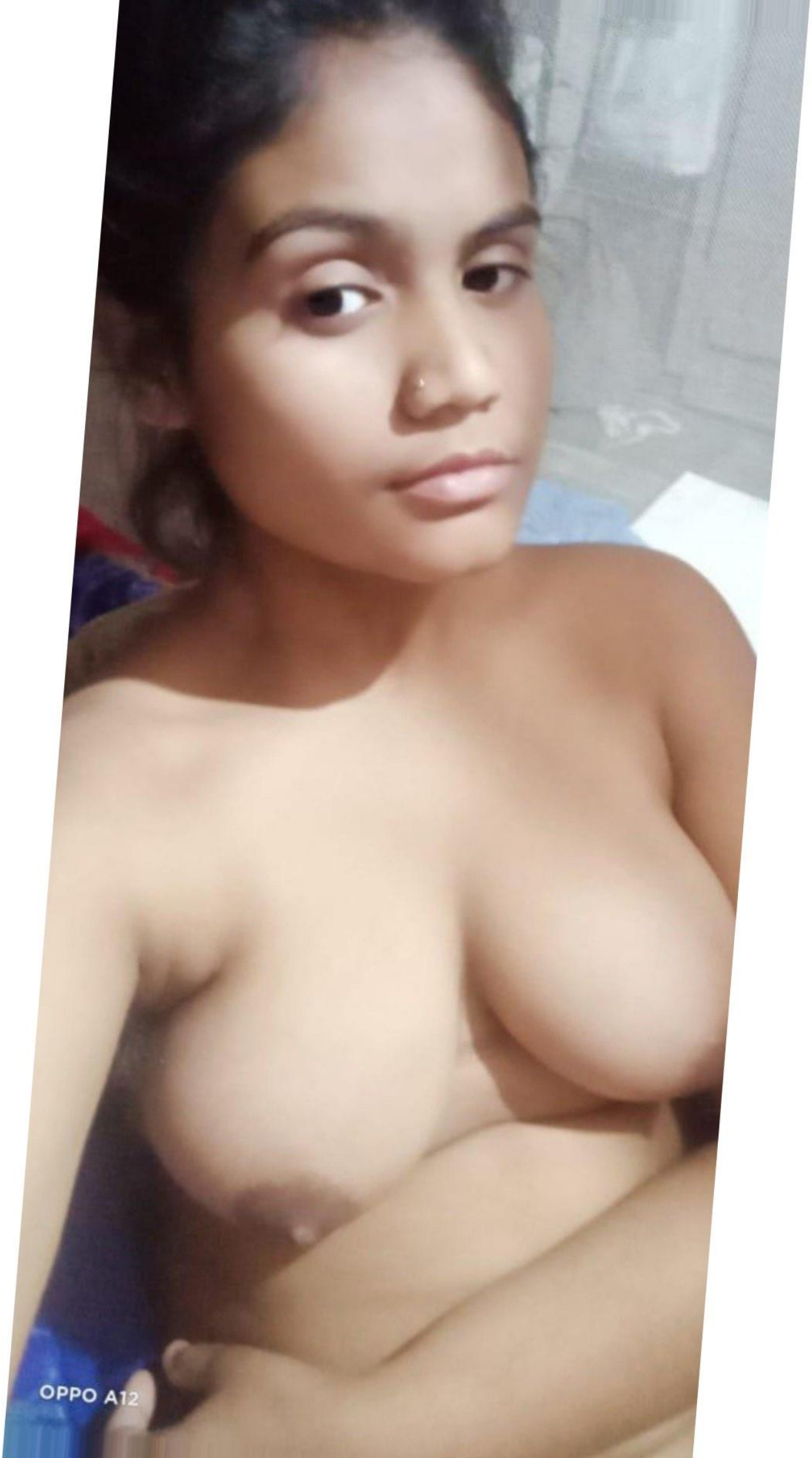
  Access control vestibule:
  - It is a small, enclosed area with two doors that creates a buffer zone between the outside environment and the secured area.
  - It typically requires individuals to pass through multiple authentication steps (such as presenting an access card or undergoing biometric verification) before they can proceed into the secured area.

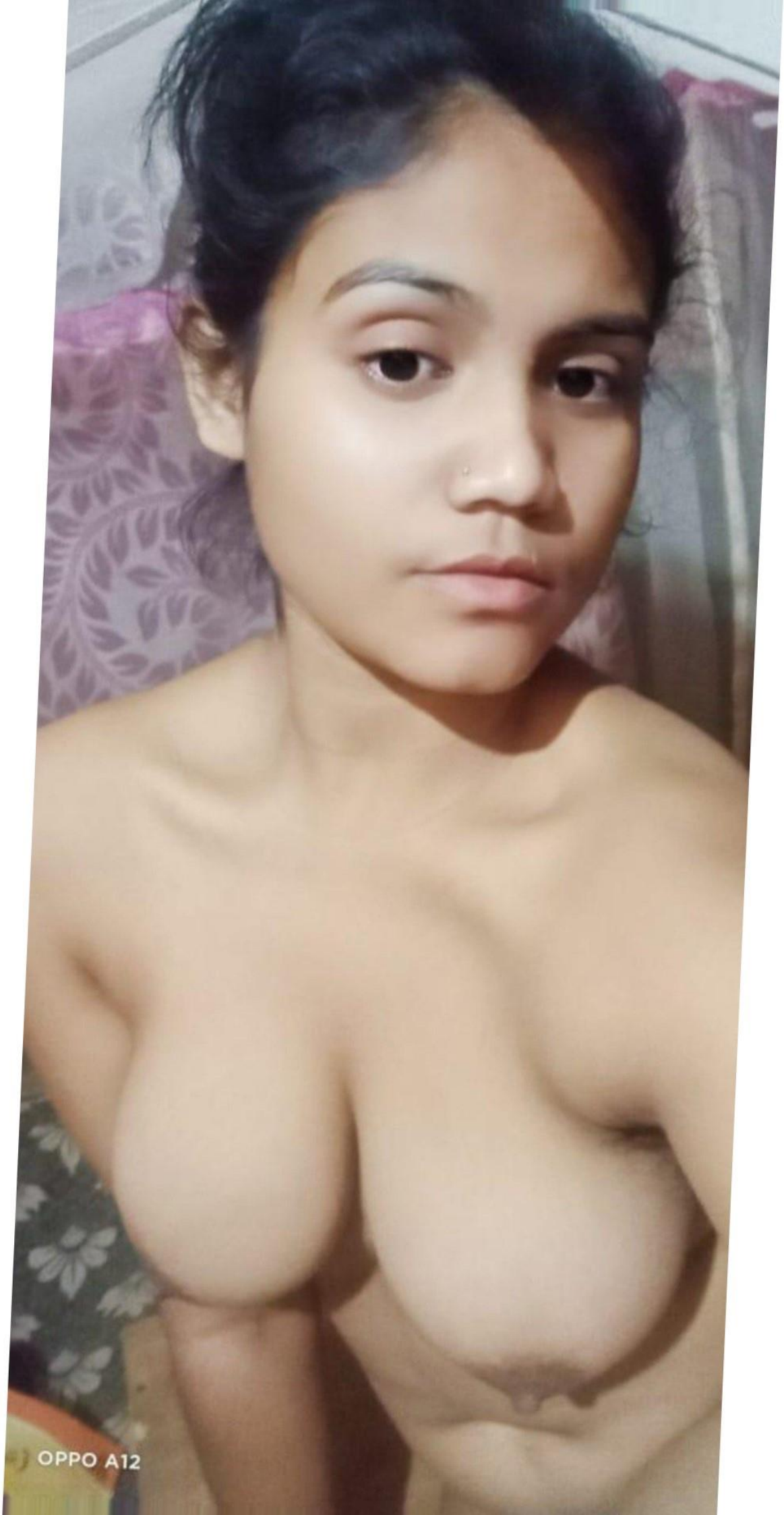
  Biometric locks:
  - These use unique physical or behavioural characteristics, such as fingerprints, iris patterns, or facial recognition, to grant access.
  - These locks scan and compare the biometric data with stored templates to verify the identity of the person attempting to gain entry.

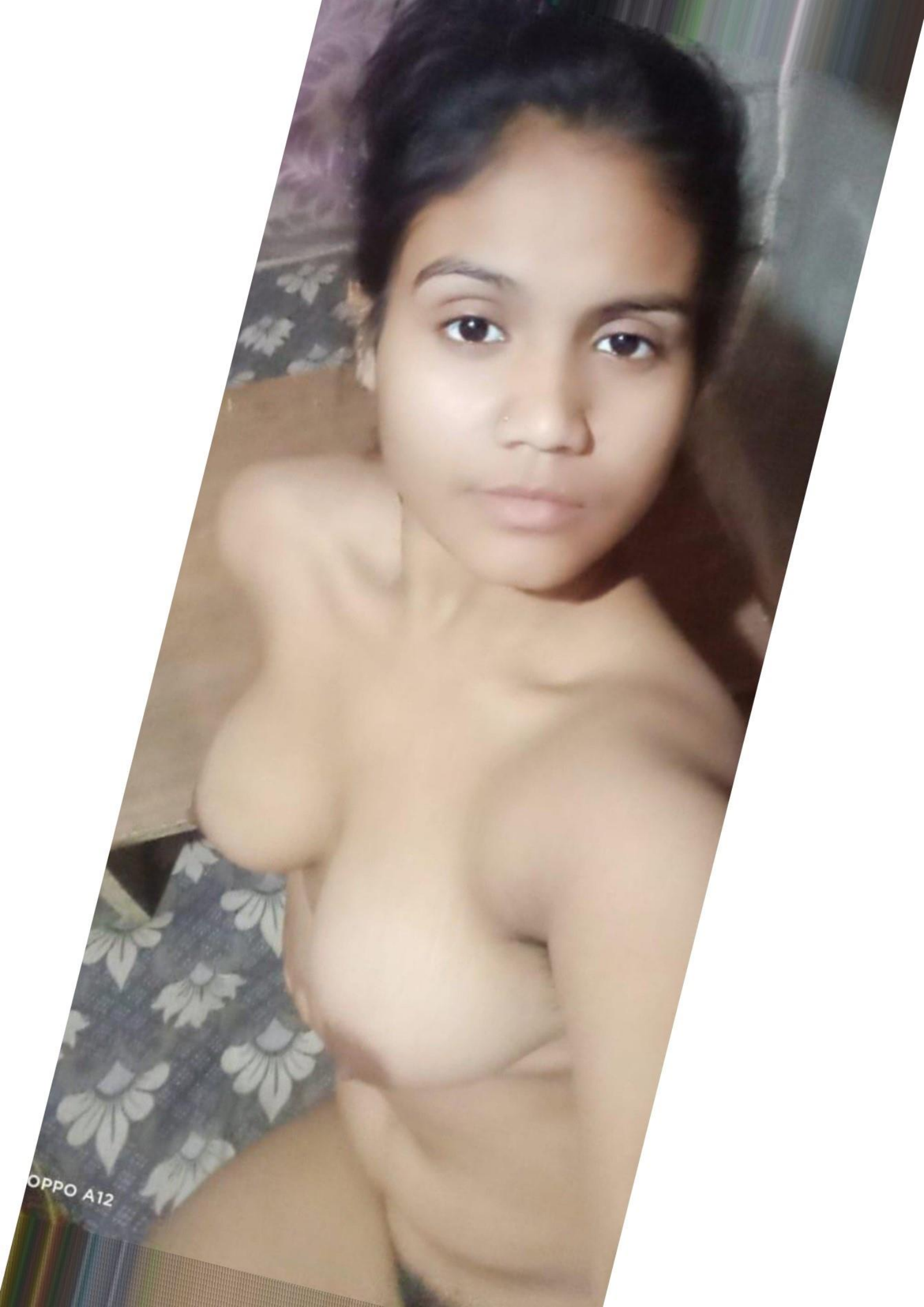
  Guards/security personnel:
  - Employing guards or security personnel is a common physical control measure. They act as a visible deterrent and can provide physical intervention and response in case of security breaches.
  - Guards are typically stationed at entry points and their responsibilities include monitoring surveillance systems, conducting patrols, and enforcing security protocols.

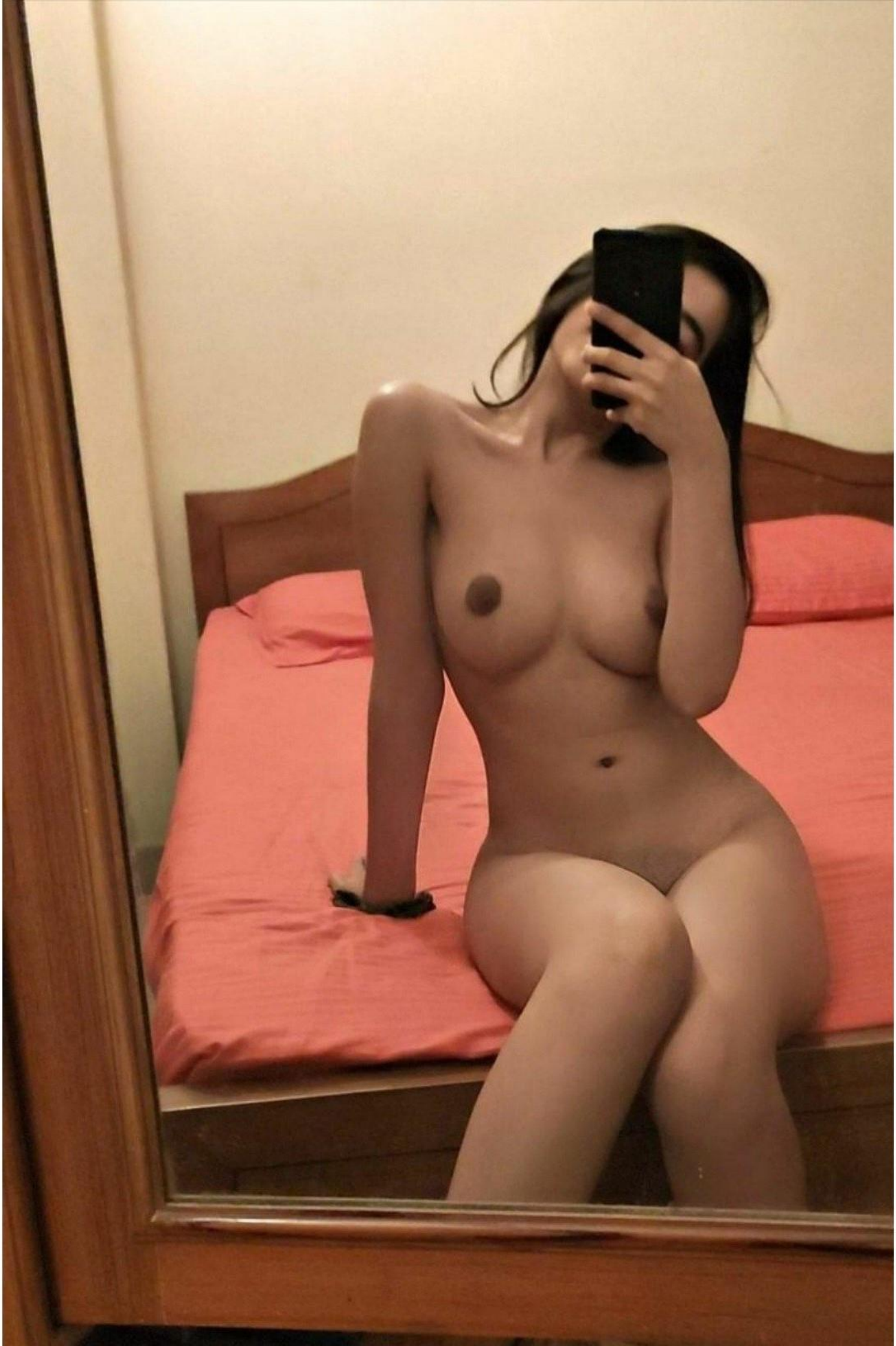
  Security fences:
  - These are used to deter unauthorized access to premises or a restricted area.
  - These fences are often made of sturdy materials such as metal or high-tensile wire, and they can be equipped with additional features, such as barbed wire or electric currents, to enhance security.

  CCTV surveillance systems:
  - Closed-circuit television (CCTV) surveillance systems use cameras to monitor and record activities in specific areas.


OPPO A12


OPPO A12


OPPO A12

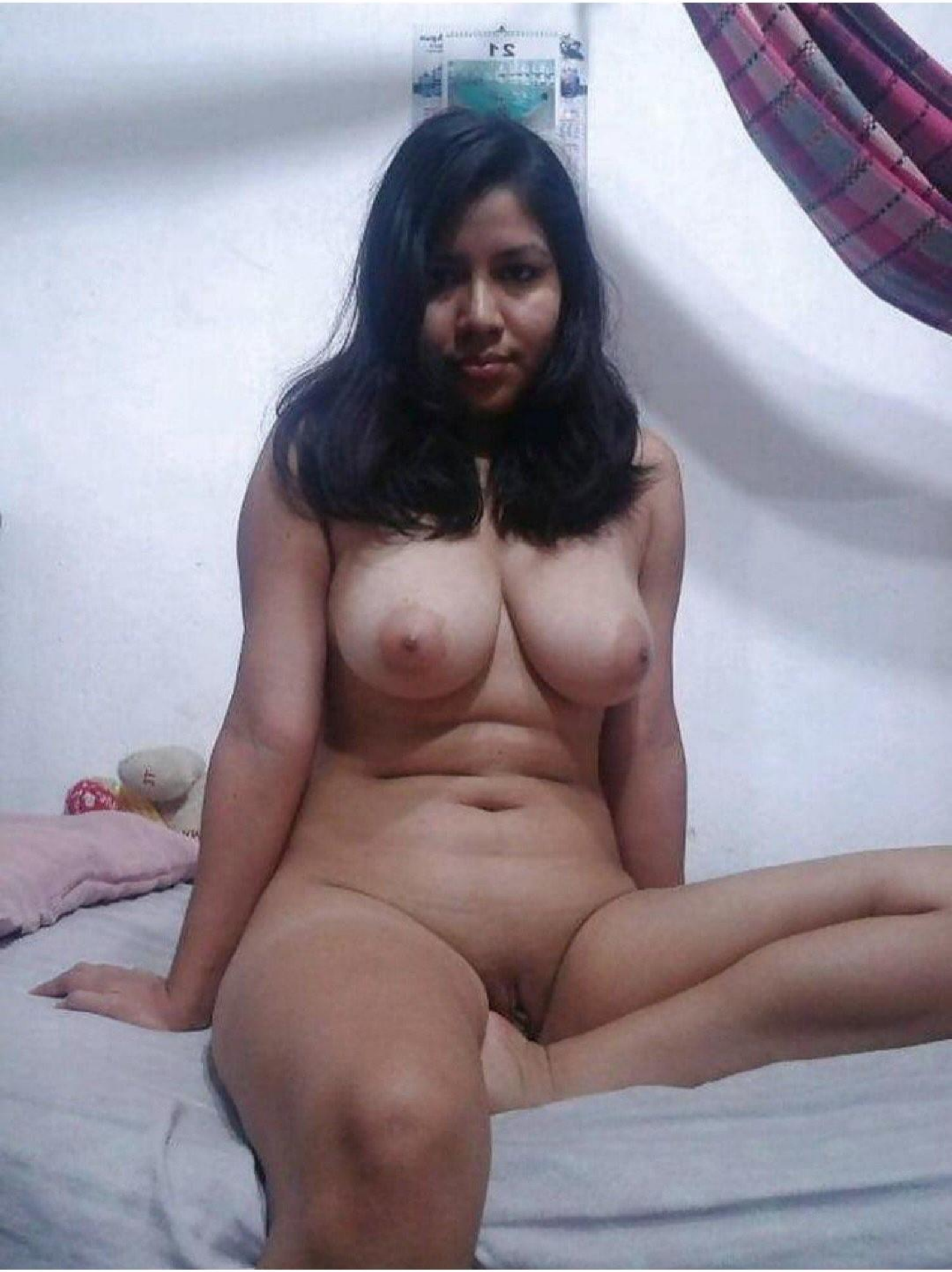


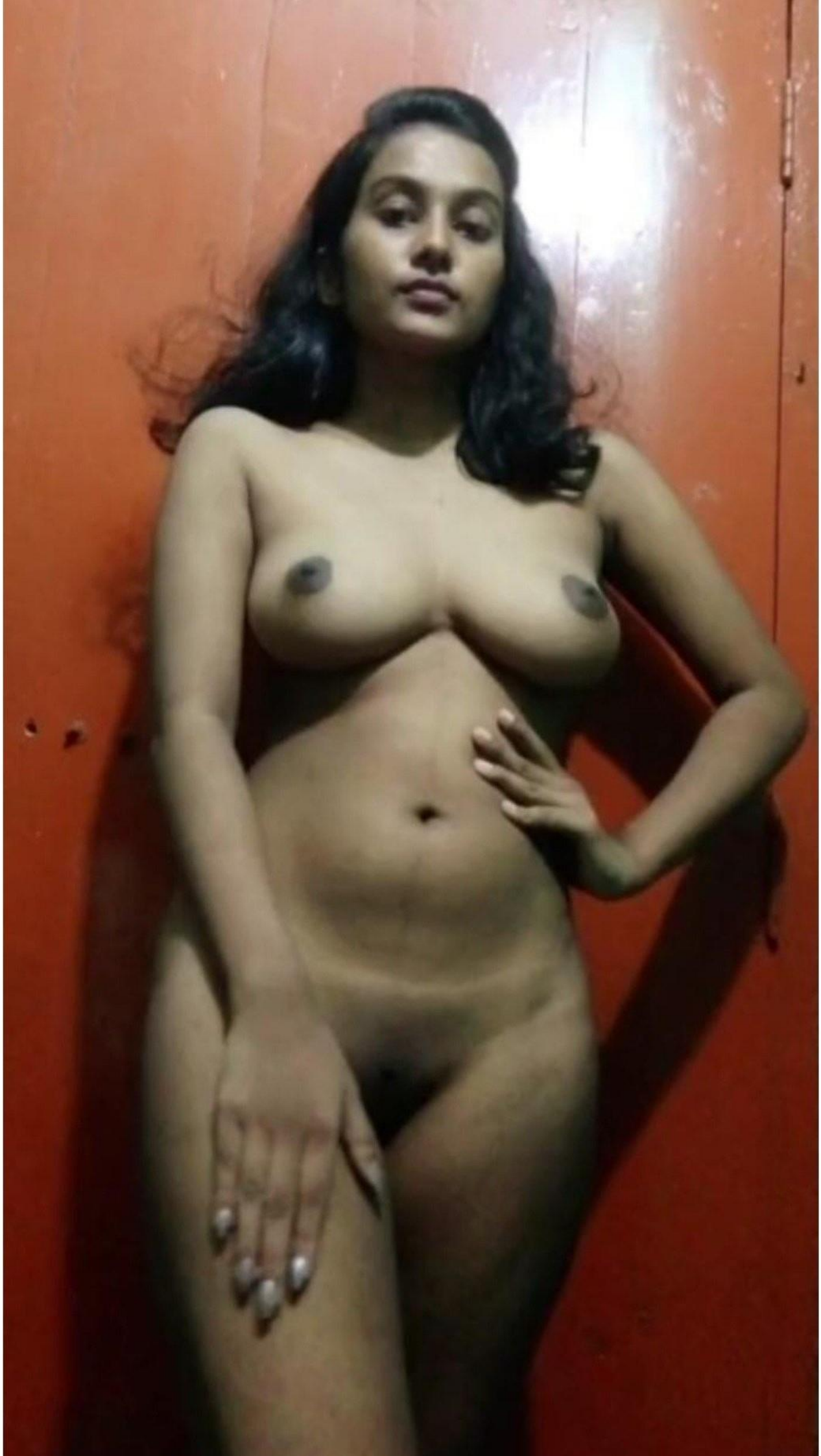

07/17/20 16:11

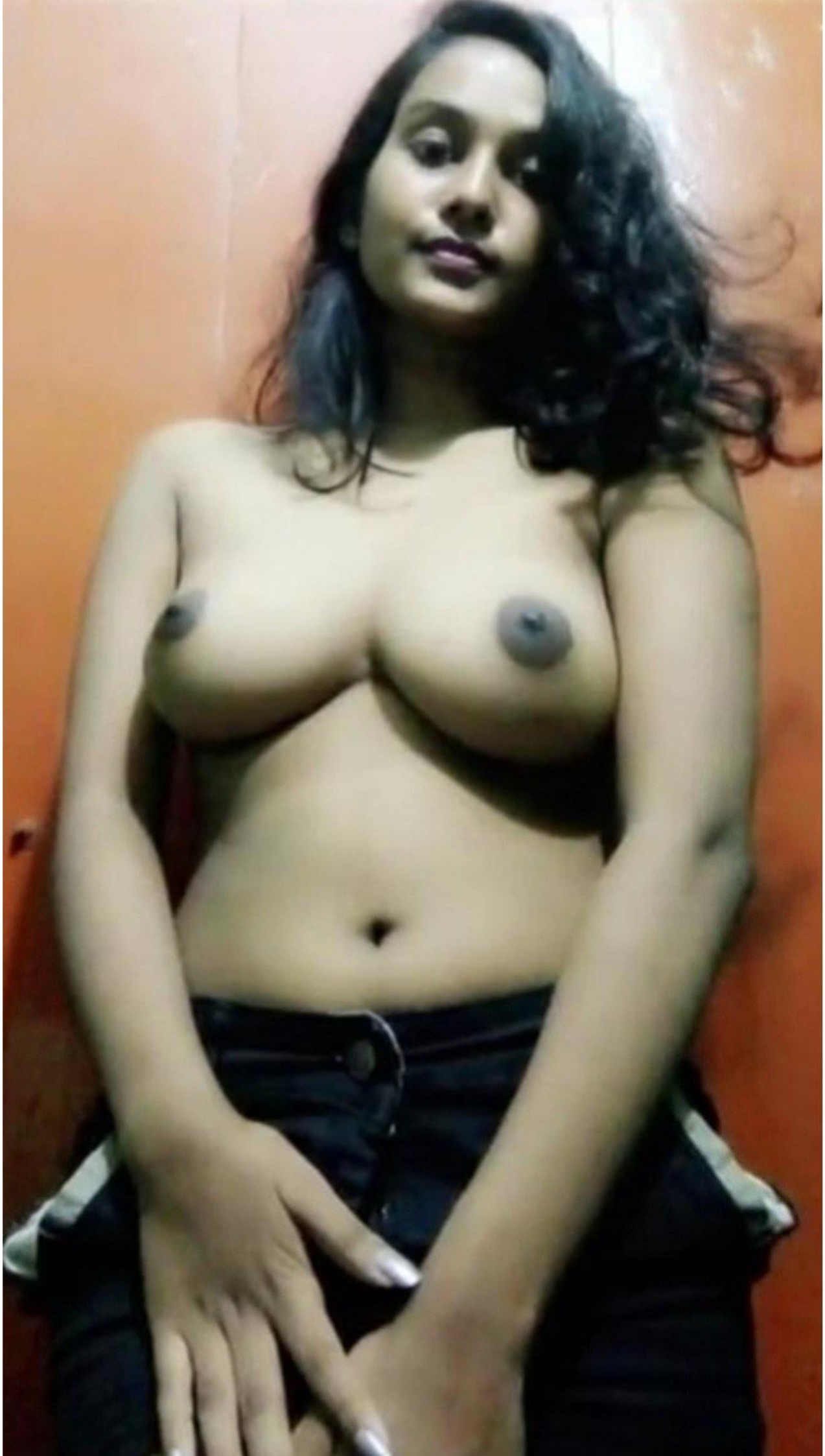
07/26/20 01:17

07/26/20 01:21

07/29/20 00:14

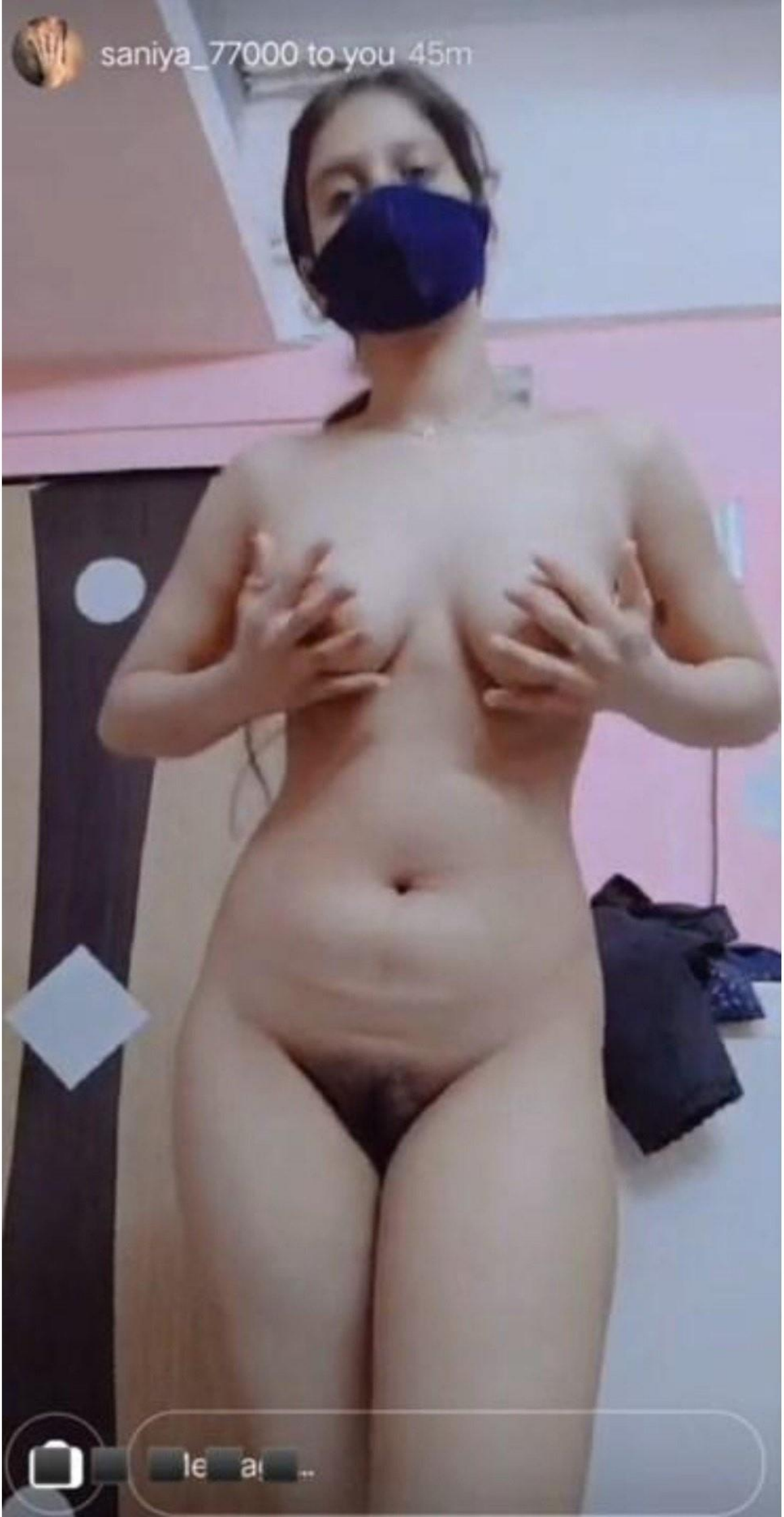


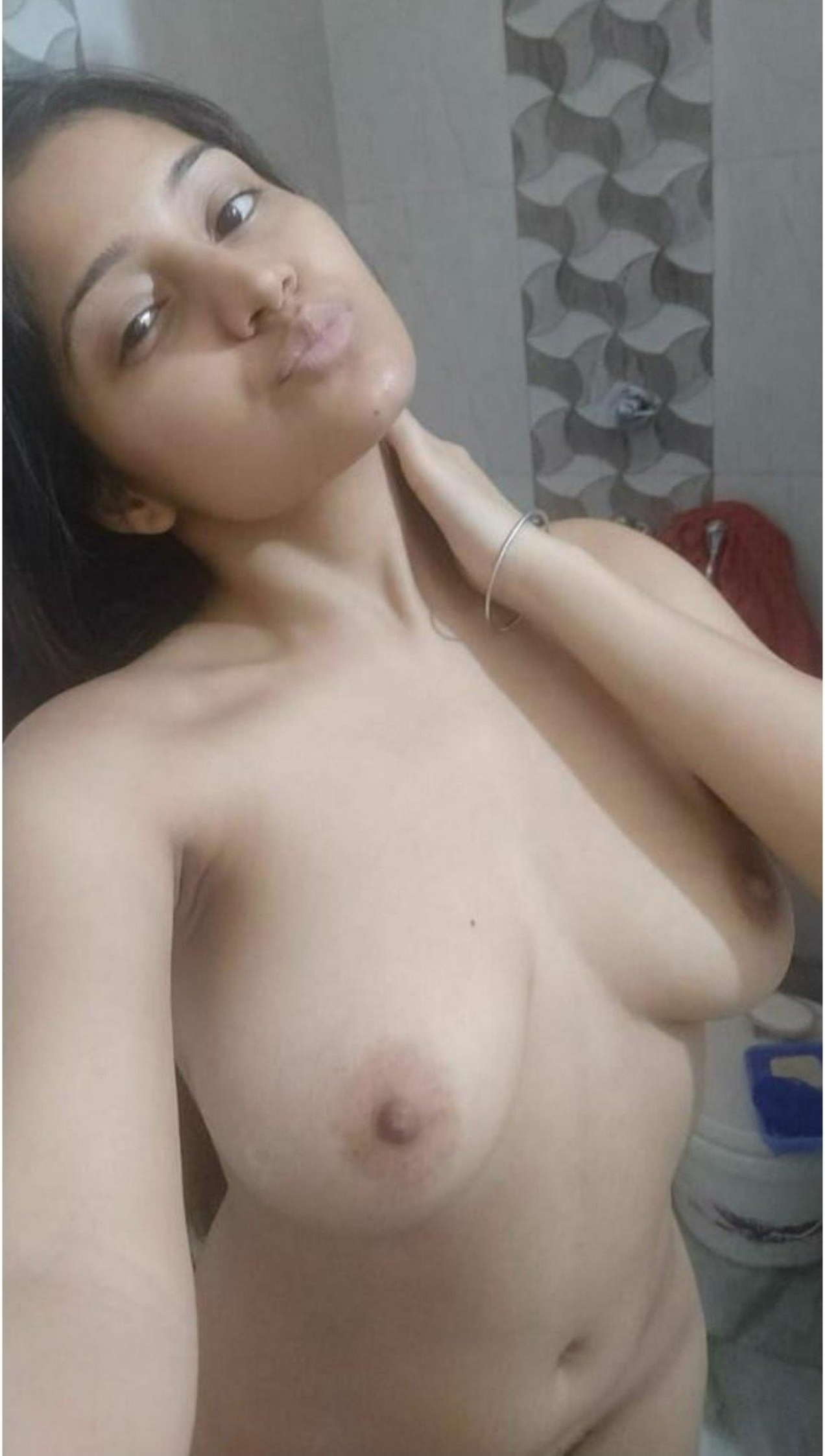




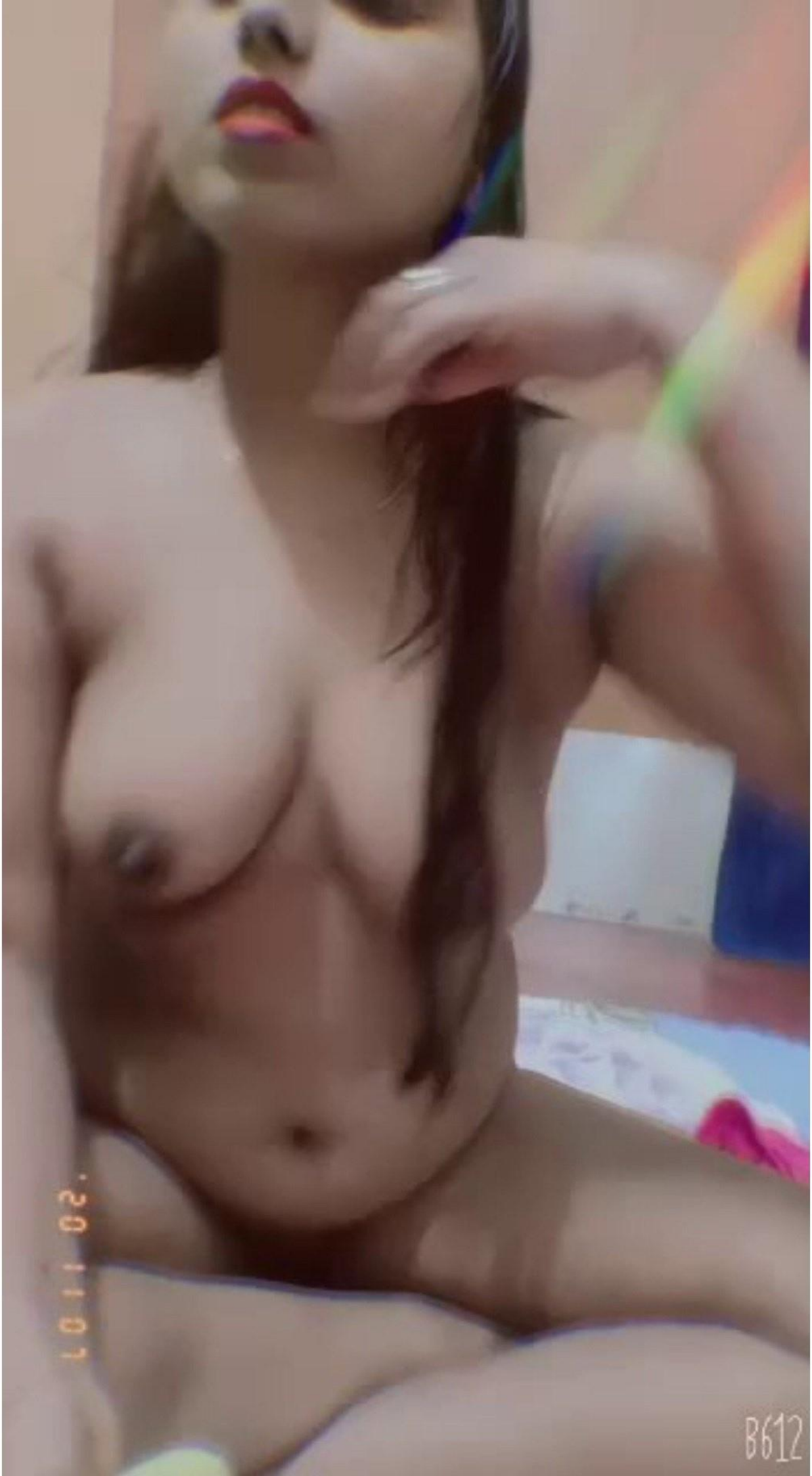

B612

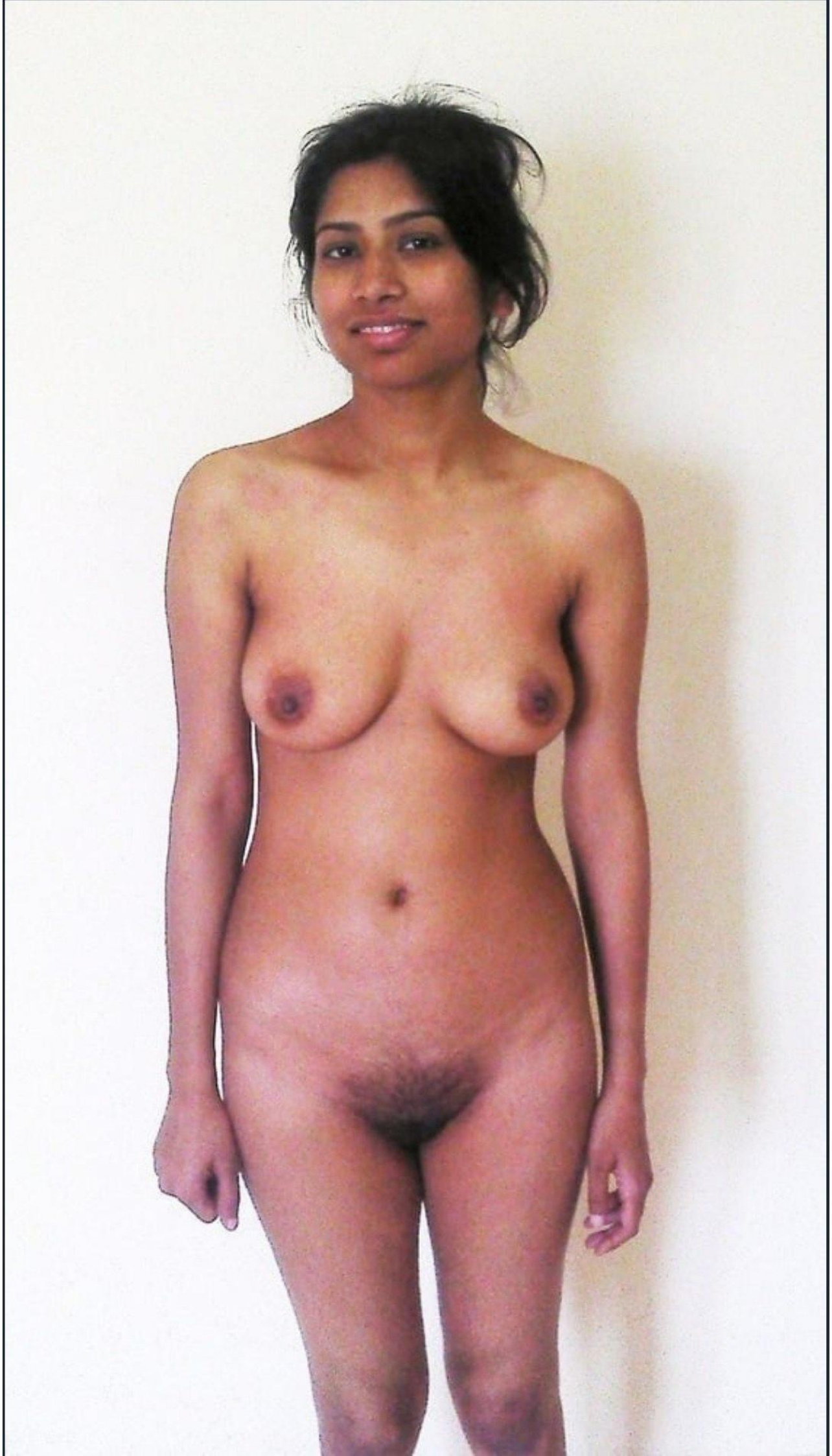

B612

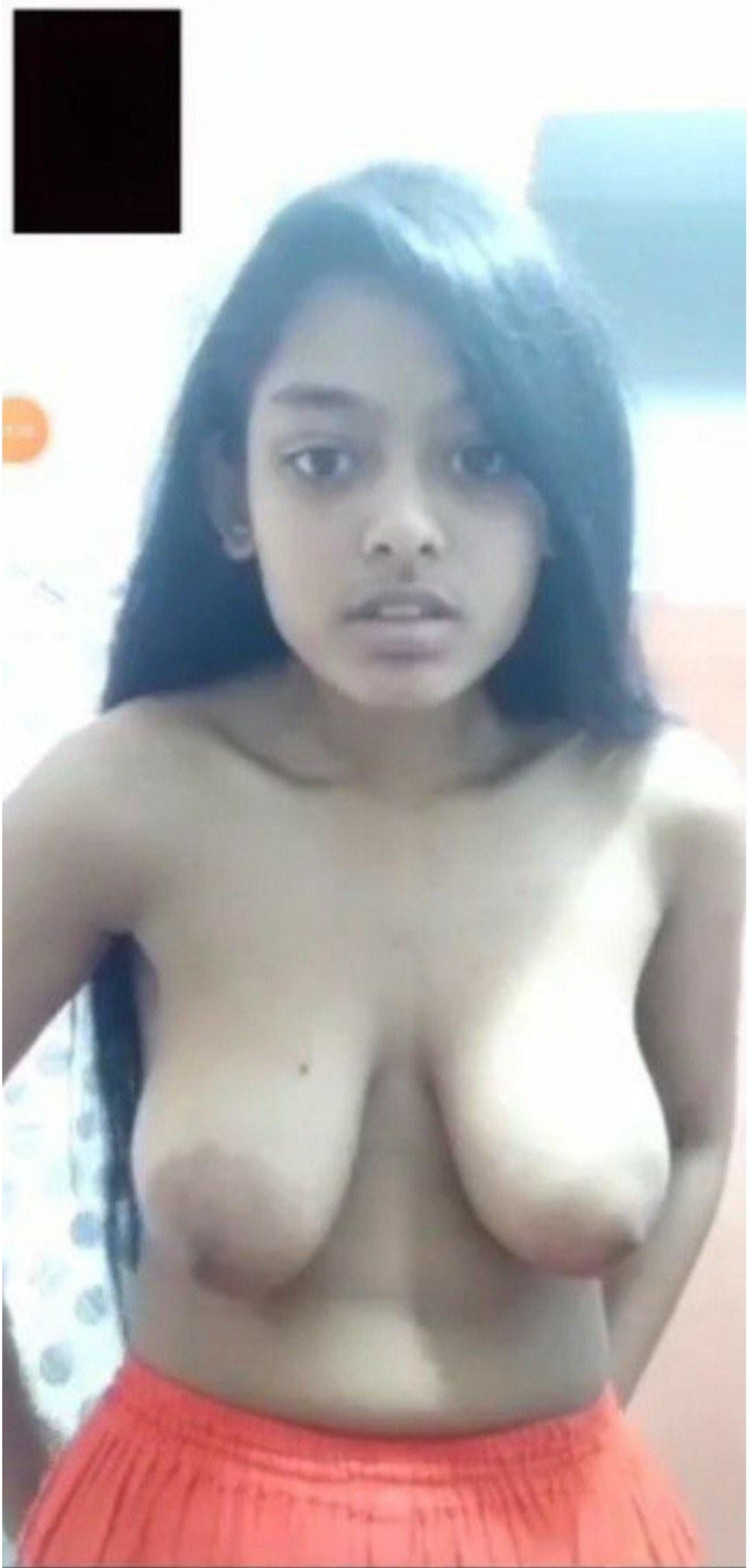

saniya_77000 to you 45m




2019.08.30 16:02


20 11 02.
B612






OnlyFans.com/brownbutte

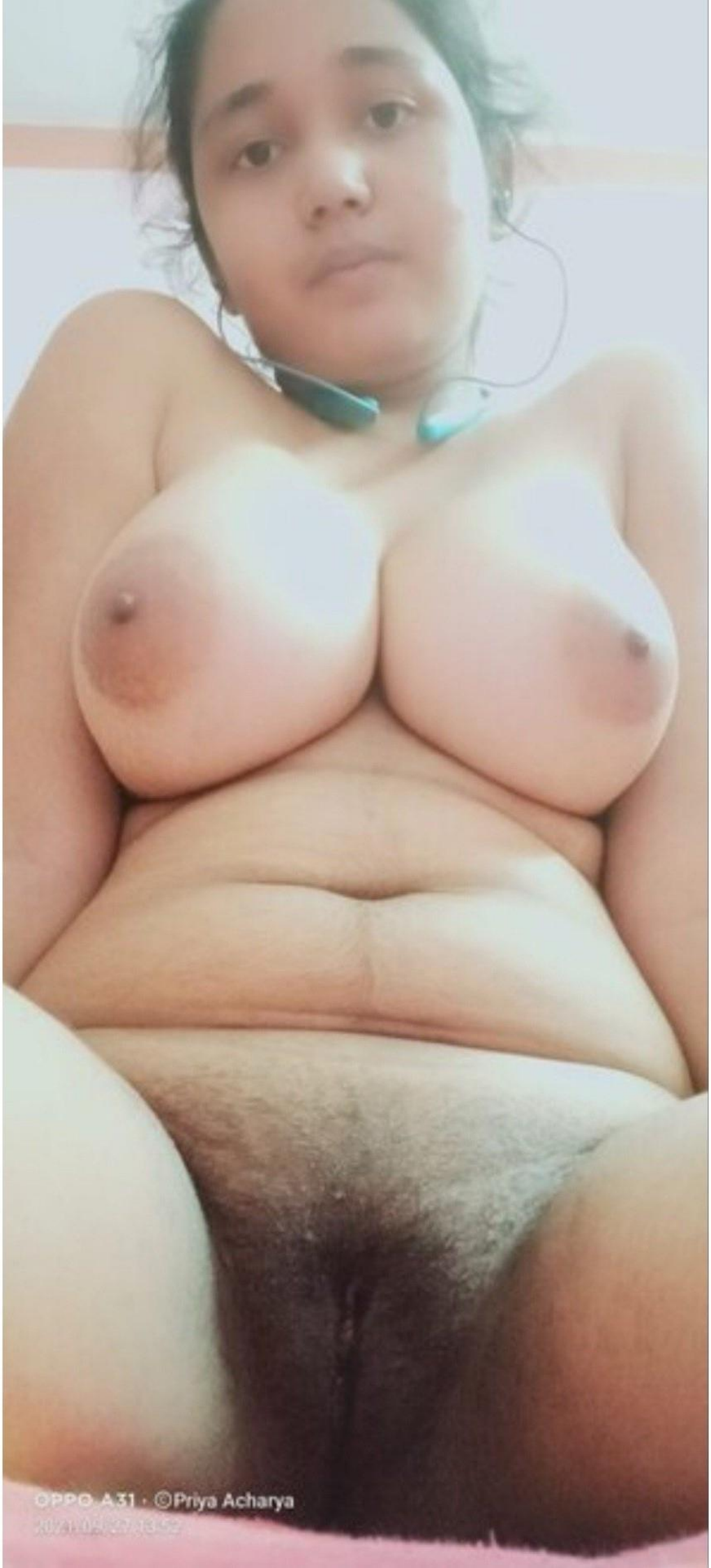

KING
WORLD HISTORY

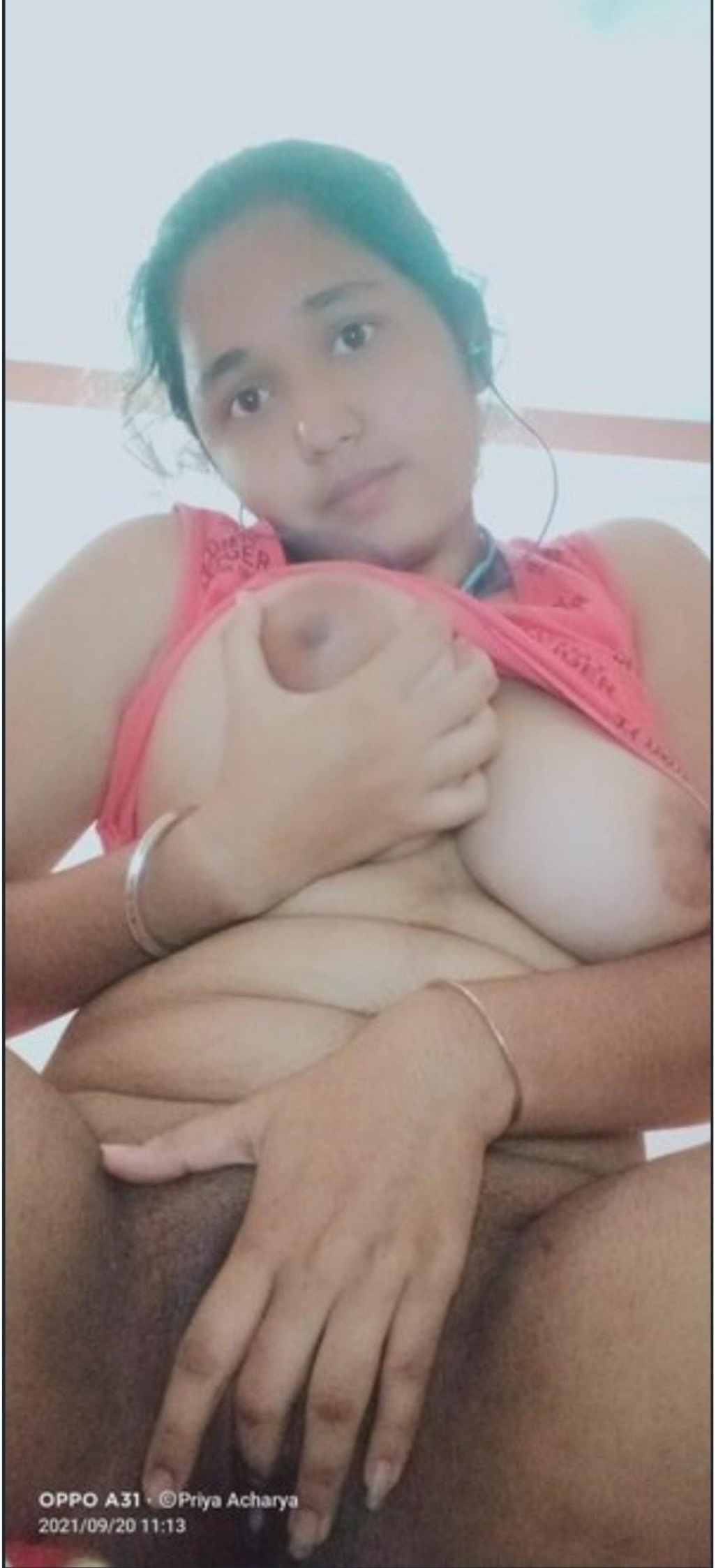
03/23/21 19:03

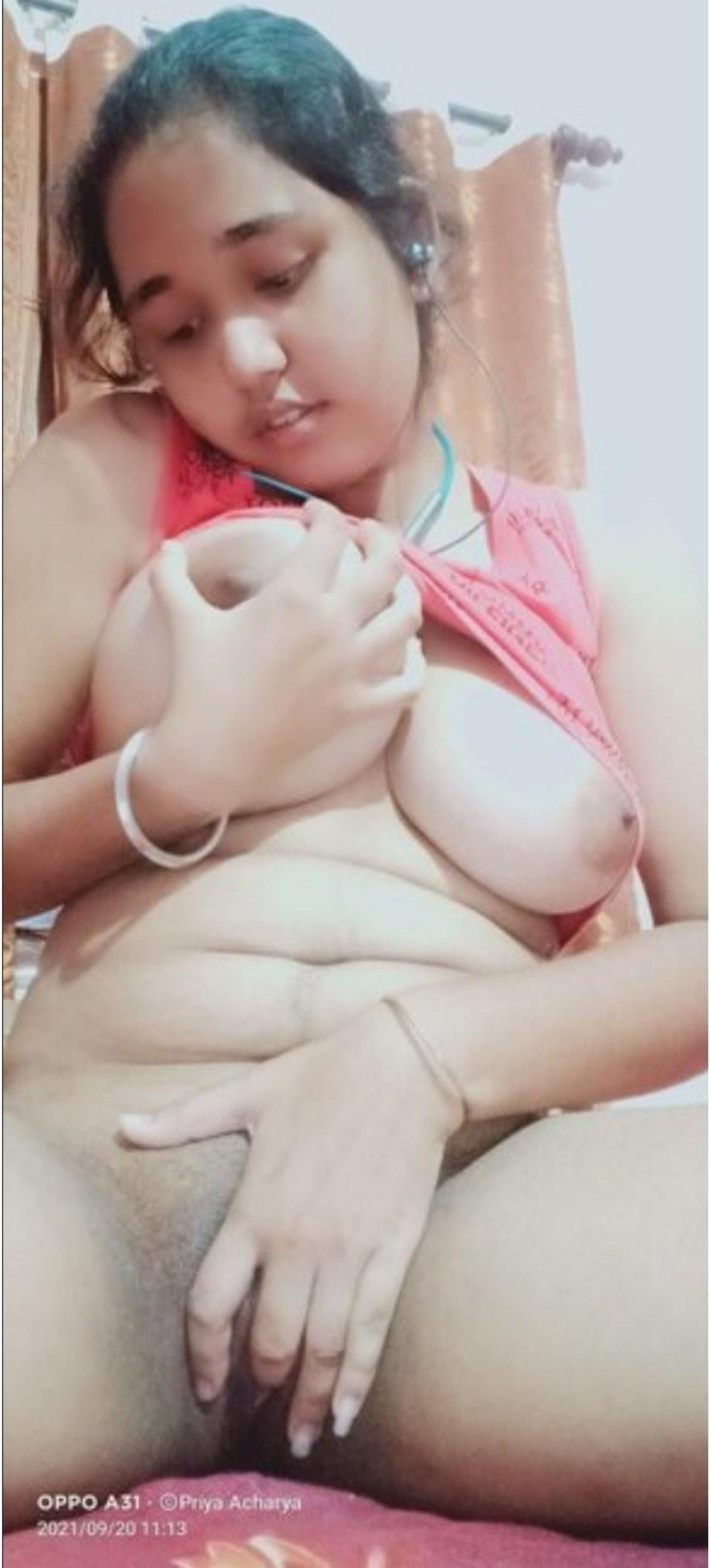

03/23/21 19:04

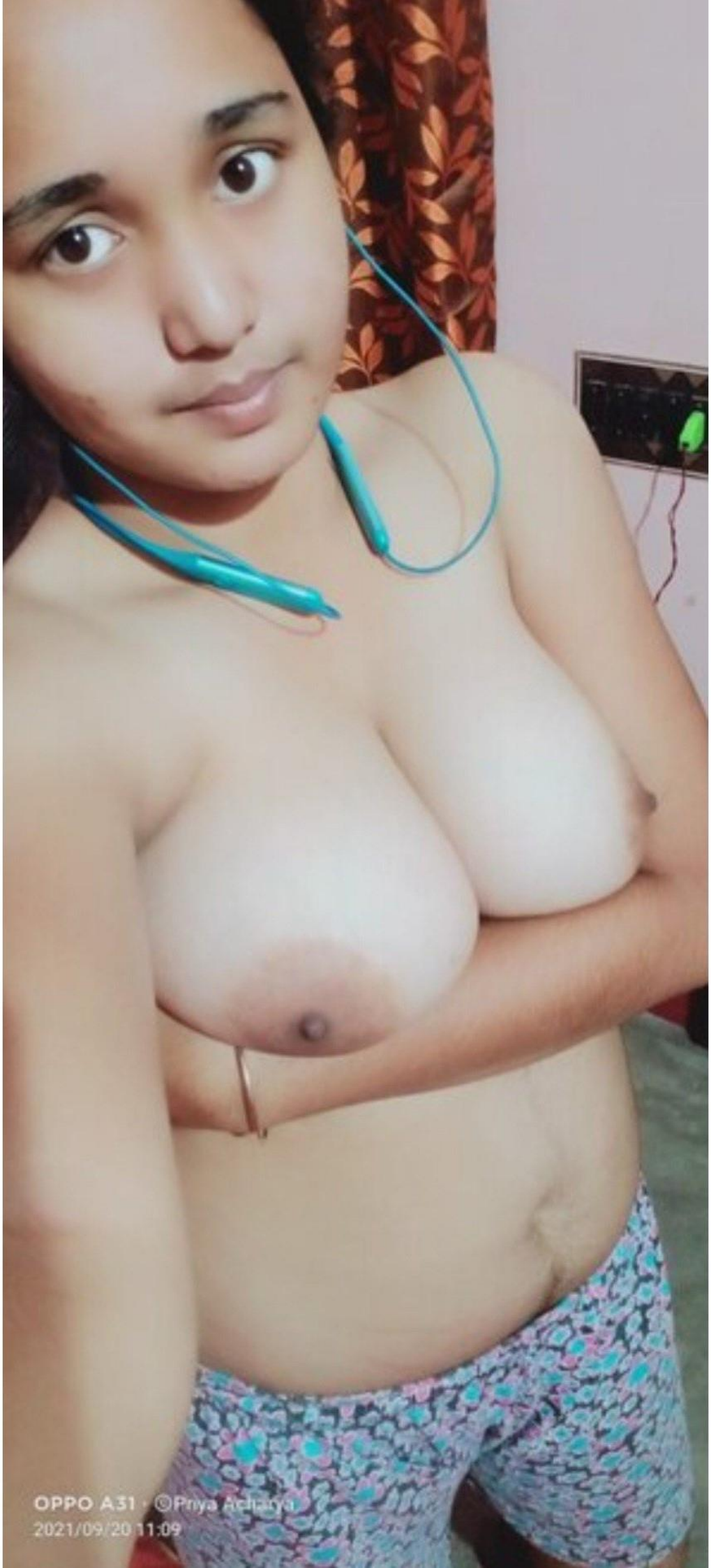
03/23/21 19:03


7/3/21 18:22

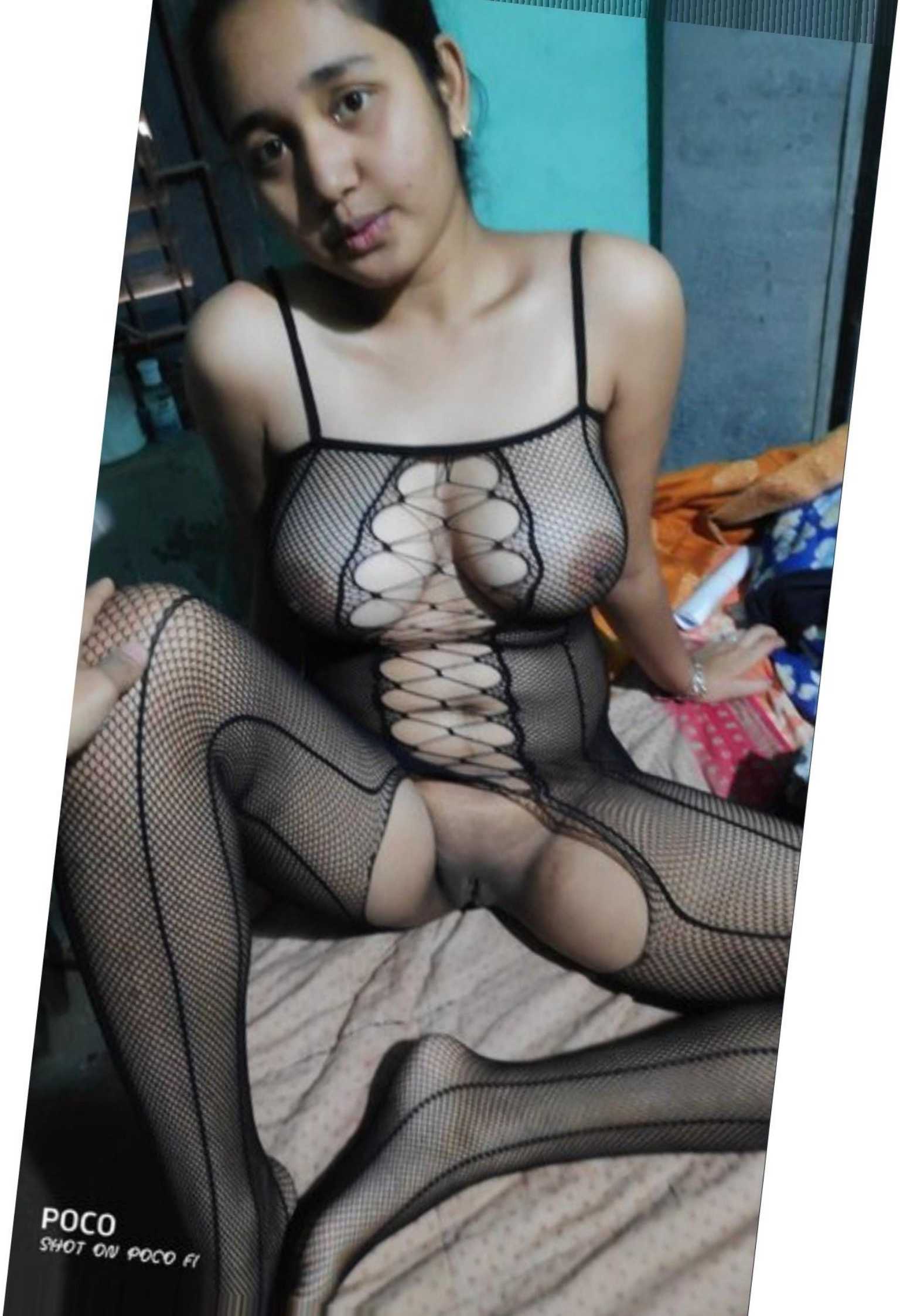

OPPO A31 · ©Priya Acharya


OPPO A31 · ©Priya Acharya
2021/09/20 11:13


OPPO A31 · ©Priya Acharya
2021/09/20 11:13


OPPO A31 · ©Priya Acharya
2021/09/20 11:09

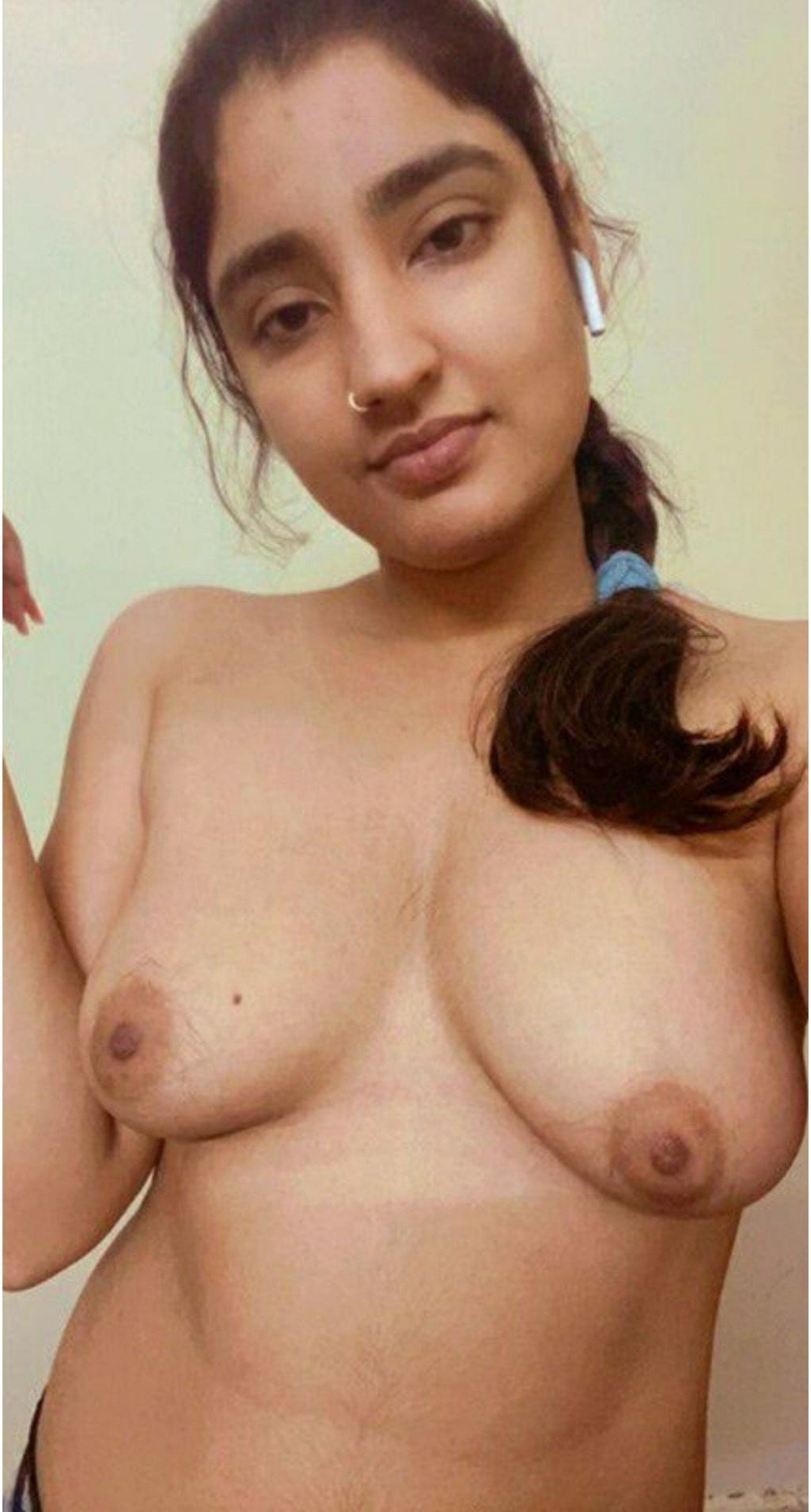

POCO
SHOT ON POCO F1

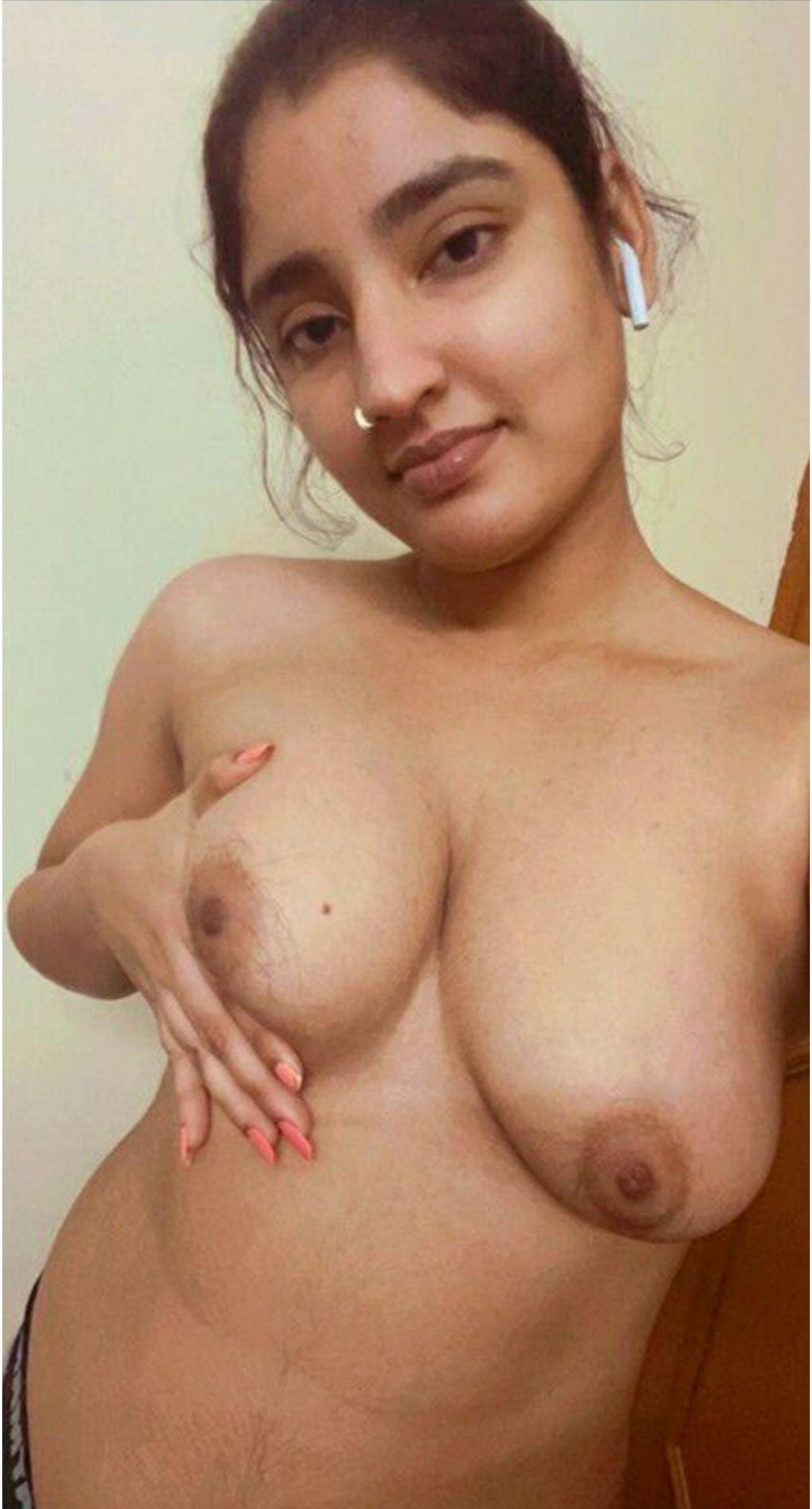

POCO
SHOT ON POCO F1

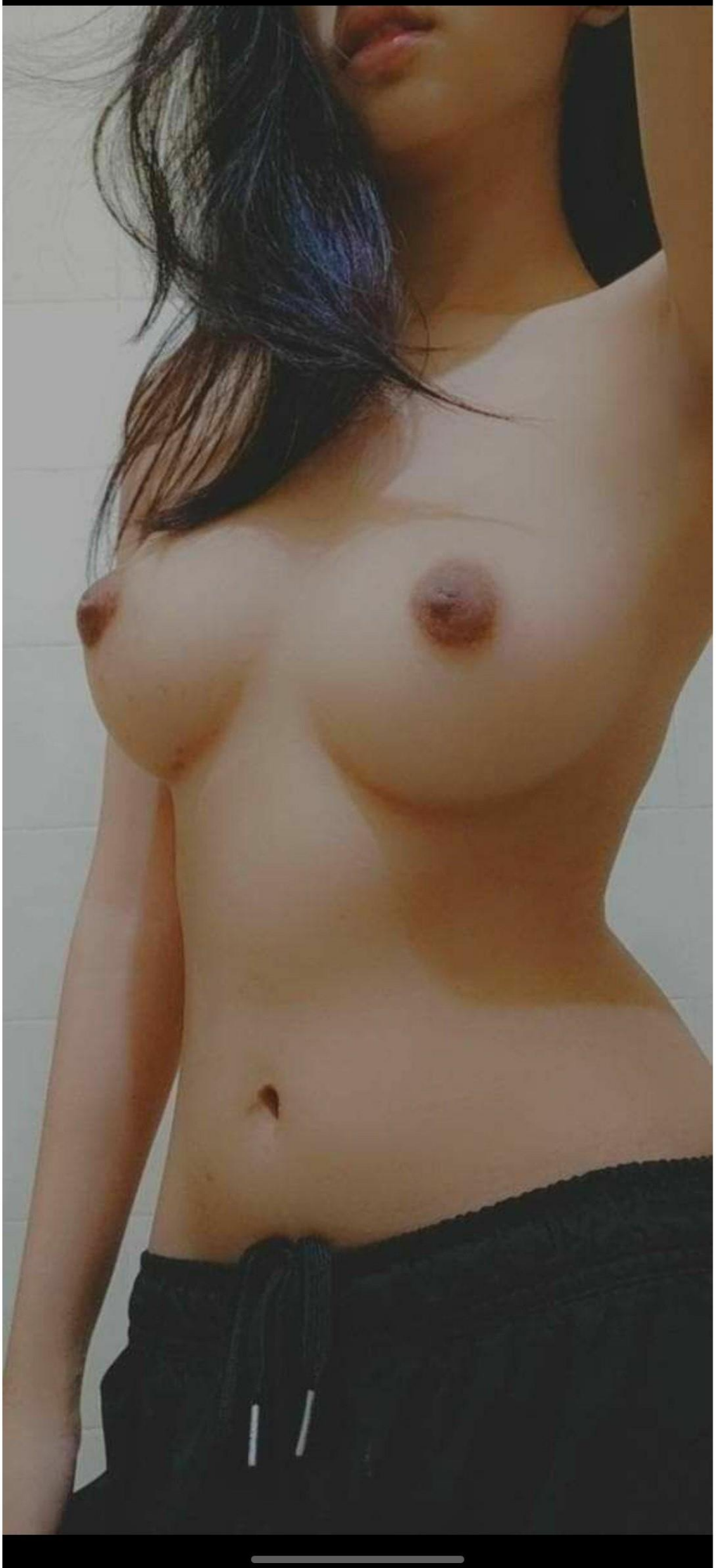

10/17/21 12:46

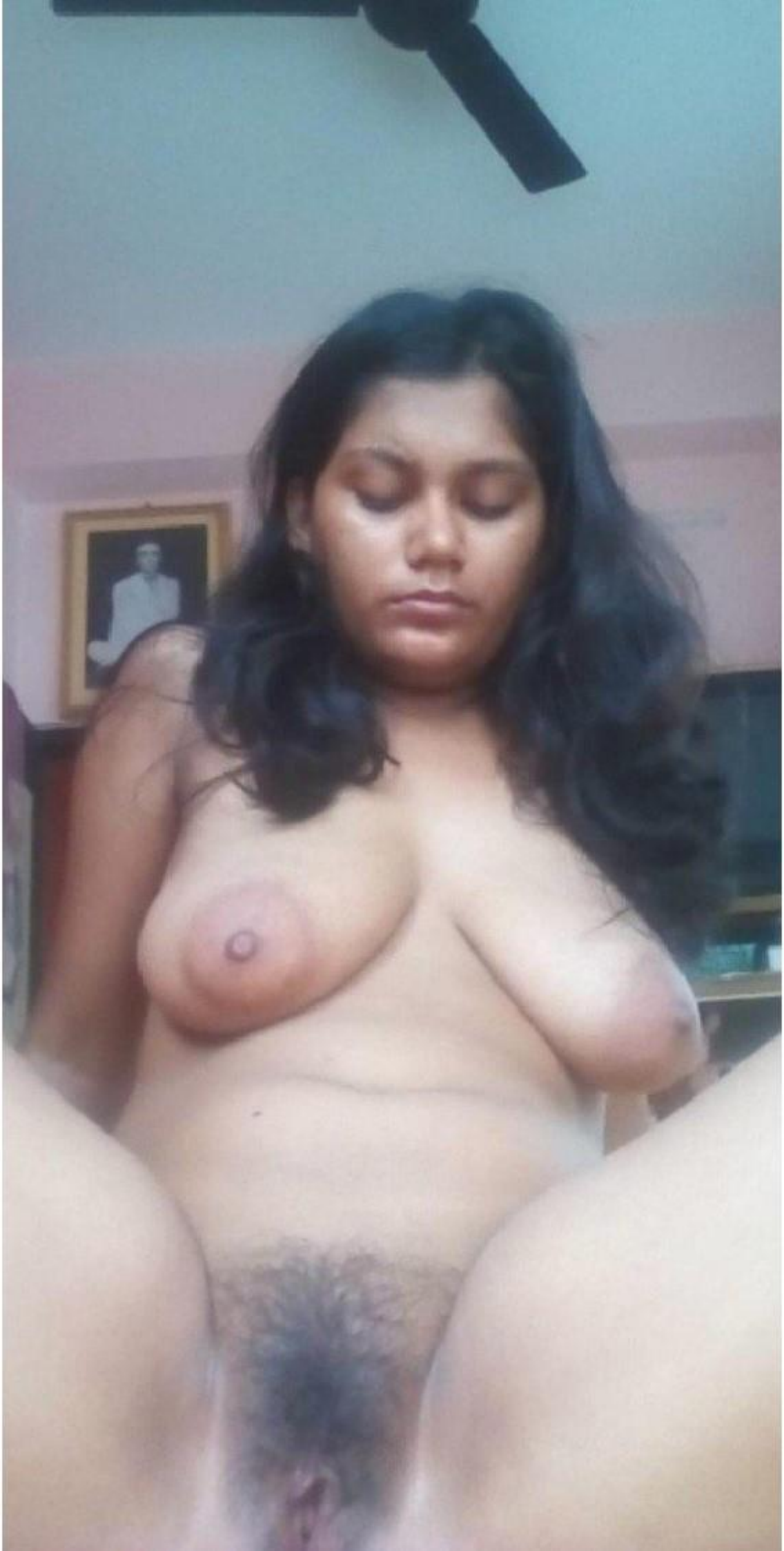
12/08/21 11:57


11/20/21 02:27





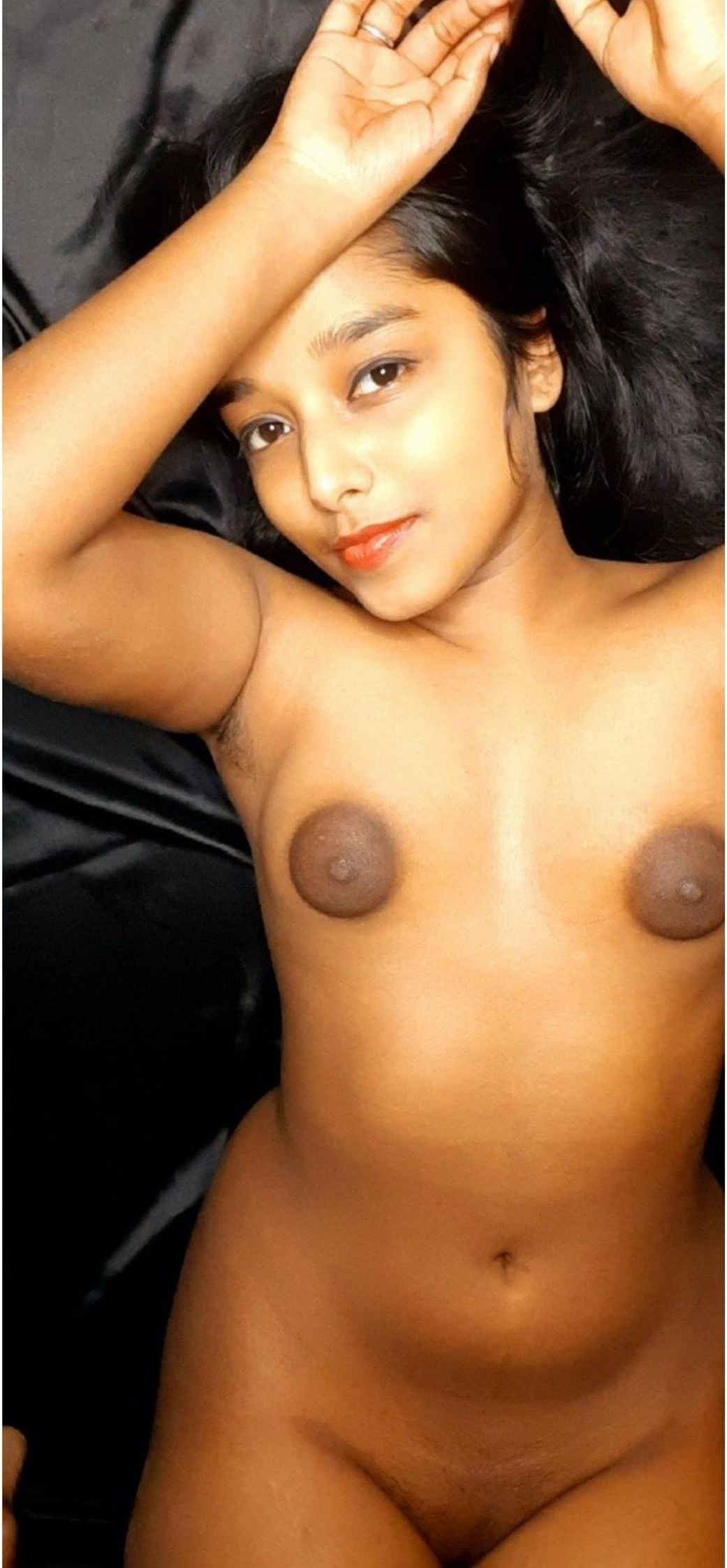





2019/4/3 17:18


2019/4/3 17:09


2019/4/3 17:13



전i寸후