

MCQ Question · mcqquestion.com

Communication Networks, Social Media and Internal Security

Free · Share

Communication Networks, Social Media and Internal Security

Communication technology has reshaped internal security in ways older frameworks never expected. The tools that connect us also create new risks, and new questions about privacy and order.

> **Arab Spring** Social media helped coordinate 2010-2011 protests.
> **Bangalore 2012** Rumours sent about 30,000 people fleeing.
> **Privacy** Fundamental right, 24 Aug 2017.
> **Deepfake rules** IT Amendment Rules, 2026.

Intermediary: A platform hosting others' content.

Deepfake: AI-faked image, audio or video.

TRAI: Telecom regulator.

Proportionality: Limit must fit its aim.

1 Chapter 1: Technology, Reach and Risk

Must Know

Expanded reach, expanded risk

- India's IT and telecom revolution expanded reach and risk at the same time.
- More people connected also means more ways for harm to spread, faster than before.

- Mobile phones, messaging apps and CCTV raise real privacy and identity questions alongside their security benefits.
- The same network that lets police coordinate a response also lets a rumour travel as fast.
- Encrypted apps and social platforms give both ordinary citizens and extremists powerful tools.
- Neither group built these tools. Both simply inherited them.
- That is why India's security planning treats communication infrastructure as a genuine security concern, not just an economic one.

The Arab Spring

- Social media helped catalyse the Arab Spring protests of 2010-2011.
- Facebook and Twitter let organisers in Tunisia and Egypt coordinate demonstrations faster than governments could respond.
- It is the clearest global example of platforms fuelling real political change.

A real Indian case: Bangalore, August 2012

- In August 2012, fake SMS messages and doctored videos warned people from the North East living in Bangalore and Pune.
- They said reprisal violence was coming, falsely tying it to unrest in Assam.
- Within four days, roughly 30,000 people fled Bangalore alone, on the strength of fabricated rumours.
- The Centre banned bulk SMS and MMS messages for a fortnight.
- It also ordered internet providers to disable the inflammatory content.
- Arrests followed for spreading the original rumours.

- Real people abandoned homes and jobs because of messages that were never true.

Remember: Viral false content can outrun any official response. The 2012 Bangalore exodus is the concrete case.

> **Quick check 1.** In 2012, rumours spread by SMS made roughly 30,000 people flee Bangalore. *(True or False?)* See answer ↓

2 Chapter 2: Media and Privacy

Good to Know

Media's double role

- Media coverage can sensationalise a threat and amplify panic beyond what the facts justify.
- The 2012 Bangalore exodus grew partly because early reporting repeated unverified rumours.
- The same media can also contain a crisis, by spreading accurate, calming information fast enough to get ahead of a rumour.
- The difference usually comes down to one habit: verify before amplifying.
- That check can come from a newsroom or from an individual sharing a message.

The Puttaswamy ruling

- Privacy became an explicit fundamental right on 24 August 2017.
- A nine-judge Supreme Court bench ruled unanimously in *Justice K.S. Puttaswamy v. Union of India*.

- The Court read privacy into Article 21's protection of life and personal liberty. See Article 21: Right to Life and Personal Liberty and The Right to Privacy and the Puttaswamy Judgment.
- The petition began as a challenge to the Aadhaar biometric identity scheme.
- The judgment settled a bigger question: whether privacy is a constitutional right at all.

The tension

- Surveillance for security reasons can clash with this settled right.
- Courts require any limit on privacy to be proportionate to its aim.
- It must also be backed by a valid law, not just administrative convenience.
- This is a repeated exam theme and a repeated news theme.

> **Quick check 2.** Privacy was declared a fundamental right in 2017 by a nine-judge bench. *(True or False?)* See answer ↓

3 Chapter 3: The Connected Threat

Great to Know

Before and after the internet

- Threats once spread by word of mouth and print.
- That took time and stayed largely local, giving authorities a window to respond.
- The internet erased that window.
- Ideas and falsehoods now travel instantly and across borders.

India’s scale

- India crossed 1.17 billion wireless subscribers by mid-2025.
- Close to a billion people are online.
- So any viral message can reach an enormous population within hours.

The state’s response

- The state now pairs traditional security measures with media-literacy and responsible-sharing campaigns.
- It has added legal deadlines too, under the 2026 IT Rules covered below.
- The 2012 Bangalore exodus, the 2017 Puttaswamy ruling and the 2026 deepfake rules are three chapters of one story.
- Related: Internal Security Threats and Regulation of Social Media Influencers.

Think it through: Think it through: security or privacy?

A government can read messages to stop a riot. But the same power can be used to watch ordinary citizens. The Puttaswamy test asks: is there a law, a real aim and a proportionate limit? That test is the balance.

4 Chapter 4: Past Papers

Exam Point of View

UPSC 2018: privacy and Article 21

- The question asked which Articles imply the right to privacy.
- The answer: privacy is an intrinsic part of Article 21 (life and personal liberty).
- The 2017 judgment read it into Article 21, paired with Articles 14 and 19.
- (Source: UPSC CSP 2018, Q92.)

CDS 2024: the Information Technology Act

- The question asked about the IT Act, 2000.
- It makes electronic signatures legally valid, like handwritten ones.
- The Act governs digital signatures and electronic records.
- (Source: CDS I 2024, Q47.)

CDS 2022: who runs telecom policy

- The question asked who implements telecom policy.
- The answer: the Digital Communications Commission, the executive side, not the regulator TRAI.

- TRAI regulates. The Commission implements policy.
- (Source: CDS II 2022, Q29.)
- Try a related question: TRAI: established by an Act of Parliament.

> **Quick check 3.** The right to privacy is an intrinsic part of Article 21. *(True or False?)* See answer ↓

5 Chapter 5: Current Affairs

Current Affairs

India's deepfake rules, February 2026

- MeitY notified the IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026.
- Platforms got just 10 days to comply before the rules took effect on 20 February 2026. (Source: Freshfields.)
- Platforms must now visibly label AI-generated images and videos.
- Takedown time for harmful content is cut from 24-36 hours to just 2-3 hours.
- This answers the "viral false content outruns any response" trap with a specific legal deadline.
- India is among the first major economies with enforceable deepfake-specific rules.

> **Quick check 4.** The 2026 IT Rules require platforms to label AI-generated content. *(True or False?)* See answer ↓

Quick Q&A

- **Arab Spring years?** 2010-2011.
- **Bangalore exodus year?** 2012.
- **Privacy ruling date?** 24 Aug 2017.
- **IT Act year?** 2000.
- **Telecom policy body?** Digital Communications Commission.

Practice MCQs

1. What has the IT and telecommunications revolution done, alongside expanding communication possibilities?

A. Only affected communication in rural areas

B. Eliminated all security risks connected to communication

C. Expanded security risks alongside those communication possibilities

D. Had no effect on internal security at all

See answer ↓

2. What dual role does media play regarding security threats?

A. It can sensationalize threats, amplifying panic, or help contain them by spreading accurate information

B. Media has no role at all in how security threats are perceived

C. Media can only ever help contain threats, never amplify them

D. Media only ever amplifies panic, with no positive role possible

See answer ↓

3. What role did social networking media play in the Arab Spring?

A. A role limited only to television broadcasting

B. A significant role in sparking the series of protests, showing how digital platforms can catalyze political movements

C. Only a role in suppressing the protests, not sparking them

D. No role at all, since the Arab Spring predates social media

See answer ↓

4. Why is content 'going viral' considered a distinctly modern security concern?

A. Viral content only ever spreads slowly, giving authorities ample time to respond

B. False or inflammatory content can spread to millions of people before authorities have any chance to respond

C. Viral content is always accurate and requires no security response

D. Going viral has no connection to security concerns at all

See answer ↓

5. Why do laws written for an earlier communication era often struggle with today's platforms?

A. Because communication laws are never affected by changing technology

B. Because those laws often don't address platforms and behaviors that didn't exist when they were drafted

C. Because new communication platforms never raise any legal questions

D. Because older laws are always automatically updated to cover new platforms

See answer ↓

Answer Key

1. **C.** The IT and telecommunications revolution has massively expanded communication possibilities. It has also expanded security risks. These risks have grown alongside the new possibilities. ↑ Q1
2. **A.** Media plays a dual role in security threats. It can sensationalize them, amplifying panic. Or it can help contain them by spreading accurate, calming information instead. ↑ Q2
3. **B.** Social networking media played a significant role. It helped spark the series of protests known as the Arab Spring. This showed how digital platforms can catalyze real-world political movements. ↑ Q3
4. **B.** Content going viral is a distinctly modern security concern. False or inflammatory content can spread to millions of people. This can happen before authorities have any chance to respond. ↑ Q4
5. **B.** Balancing digital-age free expression against security risk is a difficult, evolving challenge. Laws written for an earlier communication era often struggle. They must address platforms and behaviors that didn't exist when those laws were drafted. ↑ Q5

Quick-check answers

1. **True.** ↑ 1
2. **True.** ↑ 2
3. **True.** ↑ 3
4. **True.** ↑ 4

Curated by Arsalan Zuberi · mcqquestion.com

Scan to read online

https://mcqquestion.com/articles/communication-networks-social-media-security/