

Privacy.

1) Explain offensive speech and censorship?

Illustrate with relevant example for the importance of cyber censorship in cyberspace.

→ Offensive speech is any form of communication that hurt, insult, disrespect other based on religion, race, gender, sexual orientation or personal belief.

Include

1) Hate speech: All [religious] racial group are criminals.

2) Cyberbullying: Harassing someone repeatedly via msg or comments.

3) Trolling: Posting rude, shocking comment just to upset other.

4) Sexual harassment: Sending unwanted sexual content or msg.

5) Fake news: Spreading false info about health/election etc.

→ Censorship is the act of controlling or restricting access to content that is considered harmful, illegal or offensive.

Blocking or removing harmful or illegal content from the internet.

Importance

1) Preventing spread of Hate speech or violence
Censorship help stop the spread of content that promotes racism, terrorism or other violence

Eg: censoring terrorist or racist content shared on different public platform (like facebook, youtube to prevent increment of violence.)

- Protecting children from inappropriate content.
Shield minor from exposure to adult (violent or harm of content).

Eg: Blocking pornographic or violent website through child-safe filter to protect minor.

- To maintain National security.

Restrict the access to classified or sensitive info that could harm a country.

Eg: During the terrorist attack or conflict, government may censor sensitive info online to prevent panic or exploitation.

- To control fake news or misinfo.

Help to prevent public panic & ensure people receive accurate info. Eg: Social media platform removing false COVID-19 cure or election related misinfo to prevent public confusion.

- To prevent cyberbullying & Harassment

Remove offensive or threatening content to protect mental health & privacy.

Eg: Instagram & Fb censoring abusive comment or harmful post to protect user mental health.

Explain the concept of anonymity in cyberspace. Critically discuss its advantages and potential risk in relation to privacy & cybersecurity.

→ Anonymity means users can use the internet without revealing their real identity. In cyberspace, people can hide their name, location or other personal details while browsing, posting or communicating.

Advantages

→ Privacy protection.

User can protect their personal info from being tracked or misused.

→ Freedom of Expression.

People can share opinion or whistleblow without fear of counterattack especially in countries with censorship.

→ Security

Anonymity helps protect users from targeted attacks or harassment by hiding their identity.

Potential Risk of Anonymity

i) Cybercrime

Anonymity can be used by hackers, scammers, or criminals to hide their identity & carry out illegal activities like hacking, fraud or spreading malware.

2. Spread of misinformation

People may post false info or hate speech without accountability causing harm.

3. Difficulty in law enforcement.

It becomes harder for authorities to track and catch cyber criminals or solve online crimes.

4. Lack of Trust

Anonymous can make it harder to trust info or people online since their true identity is unknown.

5. Trolling

Some user anonymously provoke or upset others just for fun or to cause disruption.

Privacy is the right to control your personal info & decide who can access it.

Privacy is about keeping your personal info & data safe from others unless you choose to share it.

Privacy risk means the chance that your personal info or sensitive info might be exposed, shared or used without permission.

Eg: if a website accidentally share your email or location with strangers ; that's privacy risk.

Email privacy

Email privacy means protecting the content & details of your email from being seen, accessed or shared without your permission.

Confidentiality

→ Only sender and intended receiver should read the email . Other (like hacker or unauthorized people) should not access it.

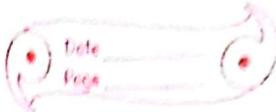
Security

Email can be protected using encryption.

Strong pw and two-factor authentication help secure email & accounts.

Data protection

Your email may contain personal data like pw, financial info or personal message . Email Service should not misuse or sell your data.



RISK

Hacking: Someone break into your email account.

Phishing: fake email trick you into revealing info

Eg: If you send your medical report to your doctor,
Email privacy issue

- No one else can read it

- The message is secure during transmission.

What is personal privacy? Explain with suitable example how technology is affecting one's personal privacy.

→ Personal privacy means keeping your personal info - like your name, address, message, photo and habits, private and under your control. It's about deciding who can see or use your info.

How affecting

Technology makes it easier to collect, store & share personal info. This can both help & harm personal privacy.

1) Data collection & Tracking

Websites, apps & devices collect data about your behaviour, preference and location often without you fully realizing it.

2) surveillance

Government or Organization can use technology to monitor people activities online or in public space through camera, internet monitoring or phone tracking.



Social Media Exposure

People often share personal moment publicly or semi-publicly which can be misused by other or lead to unwanted attention.