

SOCIETAL IMPACTS

Assignment

Case Study Questions on Digital Footprint

1. Manan, a recent college graduate, is applying for his dream job. During the interview, the hiring manager mentions they reviewed his online presence. Manan feels a pang of worry as he remembers some of his past social media posts that might not reflect well on his professionalism.

- **Questions:**

- What type of digital footprint did Manan create (active or passive)?
- How could Manan have managed his digital footprint differently to avoid this situation?

2. Sunita, a high school teacher, is very cautious about her online presence. She has no social media accounts and avoids online shopping. However, her students recently started an online forum to share class resources and discussions. Sunita is hesitant to participate because it would create a digital footprint.

- **Questions:**

- What are the potential benefits and drawbacks of Sunita participating in the online forum?
- How can Sunita manage her digital footprint while still participating in the online forum?

3. Lalita enjoys writing online reviews for restaurants and products. She believes her honest reviews are helpful to others. However, she recently received a message from a restaurant owner upset about her negative review.

- How can online reviews contribute to a person's digital footprint (active or passive)?
- What are some ethical considerations Lalita should keep in mind when writing online reviews?

4. Ashok received an email that appears to be from his bank, requesting him to update his login information. He clicks the link in the email and enters his credentials. Later, he realizes it might be a phishing scam.

- How can clicking the link in the phishing email contribute to Ashok's digital footprint (active or passive)?
- What steps can Ashok take to protect himself from phishing scams in the future?

5. Manan gave a passionate speech at a public event, and a video clip went viral on social media. While some praise his message, others criticize his stance.

- How does this situation illustrate the impact of an active digital footprint on a public figure?
- What strategies can Manan Rodriguez use to manage the online conversation surrounding his speech?

Case Study Questions on Data Protection and Intellectual Property Rights (IPR)

6. Sunita stores all her personal documents and photos on a free cloud storage service. She recently received a notification about a data breach at the company.

- What are the potential risks associated with Sunita's data storage practices?
- How can Sunita improve her data protection strategy?

7. Ashok receives an email that appears to be from his bank, requesting him to update his login information. He clicks the link in the email and enters his credentials. Later, he realizes it might be a phishing scam.

- How did Ashok's actions compromise his data protection?
- What are some red flags to watch out for in potential phishing attempts?

8. A company is considering allowing employees to use their personal devices (BYOD) for work purposes. However, they are concerned about data security risks.

- What are some security policies a company can implement for a BYOD program?
- How can employees balance convenience with data security when using personal devices for work?

9. A doctor loses their laptop containing sensitive patient data.

- What are the potential consequences of this data breach for the doctor and their patients?
- What steps should the doctor take to mitigate the damage?

10. A teenager frequently posts personal information and photos on social media.

- How can excessive social media sharing negatively impact a person's digital footprint?
- What strategies can teenagers adopt to maintain a healthy balance between online presence and privacy?

11. A small clothing company designs a unique t-shirt logo. Shortly after, a larger company releases a similar design.

- What type of IPR might be relevant in this situation (tradeMark, copyright, patent)?
- What legal options does the small clothing company have?

12. A programmer contributes code to an open-source project under the GNU General Public License (GPL). Another company uses the code to develop a commercial product without proper attribution.

- How does the GPL license protect the programmer's work in this scenario?
- What steps can the programmer take to ensure proper credit and licensing are applied?

13. The Accidental Plagiarizer: A student accidentally includes uncited passages from an online source in their research paper.

- What is plagiarism and how does it violate IPR?
- How can students avoid unintentional plagiarism in their academic work?

14. The Music Downloader: A teenager downloads music illegally from a website that does not have permission to distribute the content.

- How does this scenario violate copyright laws?
- What are some ethical and legal alternatives for accessing music online?

15. An engineer develops a new energy-saving device.

- What type of IPR would be most appropriate to protect the engineer's invention (patent, tradeManan, copyright)?
- What steps should the engineer take to secure their intellectual property rights?

Case Study Questions on Net and Communication Etiquette

16. Manan finds a funny meme online and shares it on his social media without crediting the original creator.

- **Question:** Did Manan violate netiquette? Why or why not?
- **Answer:** Yes, Manan did violate netiquette. Copying and sharing someone else's work without attribution is considered stealing intellectual property.

17. Sunita gets into a heated debate on a forum about a controversial topic. She resorts to personal attacks and insults the other person's opinion.

- **Question:** How did Sunita break the rules of netiquette in this situation?
- **Answer:** Sunita failed to be respectful of differing opinions. Net etiquette encourages respectful discourse even when there are disagreements.

18. Ashok receives an email chain mail message warning him of a dangerous online virus. He forwards the email to all his contacts without verifying the information.

- **Question:** What are the potential problems with Ashok's actions?
- **Answer:** Forwarding unverified information can contribute to the spread of misinformation online. Responsible netiquette suggests checking the authenticity of information before sharing.

19. During a video conference presentation, Ajay presents a complex topic using lengthy technical jargon. Many participants seem confused and disengaged.

- **Question:** What communication etiquette principles did Ajay potentially overlook?
- **Answer:** Ajay might have violated the principle of clear and concise communication. Effective communication involves using language that is understandable to the audience.

20. While having lunch with a friend, Emily keeps checking her phone and sending short, dismissive replies to text messages.
- **Question:** How does Emily's behaviour contradict communication etiquette?
 - **Answer:** Emily's behaviour shows a lack of respect for the person she's with in person. Communication etiquette suggests giving full attention during face-to-face interactions.
21. In an online chatroom discussion, David expresses his disagreement with another person by typing his entire message in ALL CAPS.
- **Question:** Why might David's use of all caps be considered impolite in online communication?
 - **Answer:** Typing in all caps can be perceived as shouting or yelling online, which comes across as aggressive and disrespectful.
22. Sunita constantly shares every detail of her personal life on social media, from her breakfast meals to arguments with friends.
- **Question:** What are some potential risks of oversharing on social media?
 - **Answer:** Oversharing can expose private information, create a negative online reputation, and potentially damage relationships.
23. Brian creates a fake social media profile with someone else's photos and information to deceive others online.
- **Question:** How does Brian's behavior violate social media etiquette and potentially other rules?
 - **Answer:** Brian's actions involve deception and impersonation, which are not only against social media etiquette but could also have legal consequences.
24. Ashok uses the same weak password for all his online accounts and never updates his security settings.
- **Question:** Why is Ashok's approach to security a bad idea?
 - **Answer:** Weak passwords and outdated security settings make Ashok's accounts vulnerable to hacking and data breaches. Social media etiquette encourages secure online practices.
25. In a moment of anger, Mica writes a negative post about his former employer on social media.
- **Question:** What are some potential consequences of Mica's impulsive post?

- **Answer:** Mica's post could damage his professional reputation and future job prospects. Social media etiquette suggests thinking before hitting post, especially when emotions are high.

Case Study Based Questions on Cybercrime and Cyber Laws

26. Scenario: You are a computer security consultant for a small business. The company has recently experienced a cyberattack where hackers gained access to customer data.

1. What type of cybercrime most likely occurred?

- a) Hacking for financial gain (targets)
- b) Spreading malware (uses)
- c) Cyberbullying
- d) Identity theft

2. What security measures could have helped prevent this attack? (Multiple answers possible)

- a) Keeping software and operating systems updated
- b) Using strong passwords
- c) Employing anti-virus software
- d) Downloading software from authorized websites

3. The hackers used a phishing email to trick employees into revealing sensitive information. What type of phishing attack is this most likely an example of?

- a) Smishing (text message phishing)
- b) Spear phishing (targeted email phishing)
- c) Vishing (voice phishing)
- d) Whaling (targeting high-profile individuals)

4. The stolen customer data could be used for identity theft. What Indian law would be most relevant to prosecute this crime?

- a) There is no specific law for identity theft in India.
- b) The Contract Act, 1872
- c) The Information Technology Act, 2000 (IT Act) **This act addresses cybercrimes**

5. The company wants to recover from this attack and improve its cybersecurity posture. What is the first step you would recommend?

- a) Report the attack to the police immediately.
- b) Identify the specific vulnerability that was exploited.
- c) Change all employee passwords. (While important, identifying the vulnerability helps prevent future attacks)

6. The company stores a lot of customer data. What legal requirement does the IT Act place on them regarding this data?

- a) There is no legal requirement for data storage.
- b) Data must be encrypted at rest and in transit.
- c) Data must be deleted after a set period.
- d) Customer consent must be obtained for data storage.

7. An employee claims they were not properly trained on cybersecurity best practices. How could this impact the company's legal liability?

- a) It has no bearing on legal liability.
- b) It could strengthen the company's defense in a lawsuit.
- c) It could increase the company's legal liability for the data breach.

8. The company wants to implement a security awareness training program for its employees. What topics should this program cover at a minimum? (Multiple answers possible)

- a) Recognizing and avoiding phishing attacks
- b) Importance of strong passwords and password hygiene
- c) Downloading software only from trusted sources
- d) Secure browsing practices

9. The company is considering outsourcing its data security needs to a managed security service provider (MSSP). What are some potential benefits and drawbacks of this approach?

Benefits: Expertise, cost-effectiveness (for smaller companies)

Drawbacks: Loss of some control, vendor lock-in

10. After implementing new security measures, the company wants to test its defenses. What is a safe and ethical way to do this?

- a) Hire ethical hackers to conduct a penetration test. **This is a common and safe approach**
- b) Send phishing emails to employees to see who clicks on them. (Unethical and could erode trust)

- c) Launch a denial-of-service attack against its own network. (Illegal and destructive) d) Do nothing and hope for the best.

Case-Study Based Questions on E-Waste: Hazards And Management

27. A local community is experiencing a rise in unexplained health problems, and some residents suspect it might be linked to a nearby e-waste processing facility. How could improper e-waste handling release these toxins into the environment and potentially impact the health of nearby residents?

Answer: Improper burning or dismantling of e-waste can release these toxins into the air, contaminating soil and water sources. Residents inhaling the polluted air or consuming contaminated food/water could experience health problems.

28. A family is cleaning out their garage and discovers a box of old electronics, including a CRT monitor and a non-functioning cell phone. What health risks are associated with improper disposal of these items, and how should they be disposed of safely?

Both the CRT monitor and cell phone contain hazardous materials like mercury and lead. Throwing them away with regular trash could lead to environmental contamination. They should be recycled at designated e-waste collection centers.

29. A rural community with limited waste management options resorts to burning their e-waste. Explain why this practice is particularly harmful, considering the information in the passage.

Burning e-waste releases highly toxic chemicals like dioxins and furans directly into the air. These toxins can travel long distances and cause severe health problems like respiratory illnesses, developmental issues, and even cancer.

30. A teenager buys a used laptop online at a discounted price. The laptop arrives damaged and appears to be leaking a strange liquid. What potential health hazards might this pose, and how should they dispose of the damaged laptop safely?

The leaking liquid could contain harmful chemicals like mercury or lead. Touching or inhaling these toxins can cause health problems. The damaged laptop should not be thrown away with regular trash but taken to a certified e-waste recycling facility.

31. You just purchased a brand new smartphone. What steps can you take to responsibly dispose of your old phone and minimize your e-waste footprint?

Many phone manufacturers and retailers offer trade-in programs for old devices. You can also explore certified e-waste recyclers in your area. Avoid throwing your old phone away with regular trash.

32. Some people are hesitant to recycle their old electronics due to concerns about data security. What steps can be taken to ensure personal data is securely wiped from old devices before e-waste recycling?

Most reputable e-waste recycling facilities offer data wiping services to ensure your personal information is securely removed from the device before it's recycled. You can also perform a factory reset on your device before recycling it.

33. A company is upgrading its entire computer fleet. What are some responsible options for disposing of their old computers, considering the environmental and health hazards mentioned in the passage?

The company should explore certified e-waste recycling companies that ensure proper dismantling, material recovery, and safe disposal of e-waste components. Bulk e-waste recycling programs are often available for businesses.

34. A local school wants to organize a campaign to educate students about the dangers of e-waste and promote responsible disposal practices. What key points should the campaign highlight, based on the information provided?

The campaign should emphasize the health hazards associated with improper e-waste disposal, highlight safe recycling options, and encourage students to reduce, reuse, and recycle electronics whenever possible.

35. A local electronics store is considering launching a take-back program for old electronics. What are some potential benefits of such a program for the store, the community, and the environment?

A take-back program allows the store to responsibly manage e-waste generated from their products. It benefits the community by providing a convenient and safe way to dispose of old electronics and reduces the environmental impact of e-waste.

36. Developed countries often export their e-waste to developing countries for processing. What are some potential problems associated with this practice, considering the health risks mentioned in the passage?

Developing countries may not have adequate infrastructure for safe e-waste processing, leading to environmental contamination and health problems for local populations. This practice should be discouraged, and responsible e-waste management solutions should be implemented globally.

Case-Study Based Questions on Cybercrime and Cyber Laws

37. A user clicks on a suspicious link in a text message and now their phone seems sluggish and displays unusual pop-up ads. What type of cybercrime might this be, and what steps can the user take to address the situation?

Answer: This could be a malware infection. The user should run a scan with their antivirus software and consider a factory reset if the issue persists.

38. Someone finds a great deal on a new laptop online but the website seems unfamiliar. How can they identify potential spoofing scams and protect their personal information?

Answer: They should be cautious of deals that seem too good to be true. Verify the website's legitimacy through independent searches and avoid entering personal information on unfamiliar sites.

39. An employee receives an email that appears to be from their bank requesting login credentials to verify a recent transaction. What red flags should they look for to identify potential phishing attempts?

Answer: The email might have grammatical errors, an urgent tone, or a sender address that doesn't match the bank's official domain. Never click on links or provide login information through emails; log in directly to the bank's website to verify any concerns.

40. A teenager is being harassed online through social media with hateful messages and rumors. What is considered cyberbullying, and what steps can the teenager take to address the situation?

Answer: Cyberbullying involves sharing negative or harmful content about someone online. The teenager should report the abuse to the social media platform and consider collecting evidence (screenshots) to potentially involve law enforcement.

41. A user struggles to remember complex passwords for multiple online accounts. How can they balance strong password security with user convenience?

Answer: Password managers can be used to store and generate strong passwords for different accounts. Multi-factor authentication can add an extra layer of security without needing to remember numerous complex passwords.

42. A small company hasn't updated their computer software and operating systems in over a year. What security risks are they facing, and how can they improve their cybersecurity posture?

Answer: Outdated software is vulnerable to known exploits. They should prioritize updating all software and operating systems to the latest versions to address security vulnerabilities.

43. A student downloads a free movie from an unauthorized website and their computer crashes soon after. What potential consequences might this hold, and where can they find safe and legal downloads?

Answer: The downloaded file could have contained malware that infected the computer. They should stick to official app stores and reputable websites for downloading software and media.

44. An international company operates a social media platform but hasn't familiarized itself with the Indian IT Act. Why is it important for them to understand this act, and what aspects might be most relevant?

Answer: The IT Act outlines cybercrime regulations in India. Understanding the act helps ensure their platform complies with Indian law, especially regarding data privacy and user protection from cybercrime.

45. A company wants to implement a BYOD policy but is concerned about potential security risks. What measures can be implemented to mitigate these risks within a BYOD program?

Answer: The company can require strong password policies, device encryption, and security awareness training for employees using personal devices for work.

46. **Beyond Antivirus:** A company relies solely on antivirus software for their cybersecurity. What are the limitations of this approach, and what additional security measures can be implemented for a more comprehensive defense?

Answer: Antivirus software primarily detects known threats. A layered security approach is recommended, including firewalls, intrusion detection systems, regular security audits, and employee training to address emerging cyber threats.