Module 5: Issues in Ecommerce

Understanding Ethical, Social and Political issues in E-Commerce:

Understanding the ethical, social, and political issues in ecommerce is crucial as online transactions and digital interactions become increasingly integral to modern life. Here's an overview of these issues:

Ethical Issues:

1. Privacy and Security: Privacy Concerns: Collection, storage, and use of personal data without consent.

Security: Vulnerabilities in transactions, data breaches, and cyber security threats.

2. Consumer Protection: Ensuring truthful representation of products and services, dealing with fraudulent activities like online scams and phishing.

3. Fairness: Addressing issues of price discrimination and unfair pricing practices, ensuring fair competition among businesses, especially small enterprises versus large corporations.

4. Intellectual Property: Protecting copyrights and trademarks in digital content and products, dealing with issues like digital piracy and unauthorized copying.

5. Online Reviews and Ratings: Fake review, paid endorsements or manipulation of ratings can deceive consumers and undermine trust in e-commerce platforms. Maintaining the integrity of online reviews and ratings systems by preventing fraudulent practices is essential for ethical for ethical business conduct.

Social Issues:

1. Digital Divide: Disparities in access to technology and the internet among different socioeconomic groups, impact on opportunities for education, employment, and social inclusion.

2. Impact on Local Businesses: Effects of ecommerce giants on local economies and traditional brick and mortar businesses, challenges faced by small businesses to compete in the digital marketplace.

3. Consumer Behaviour: Shifts in purchasing habits and the rise of impulse buying, impact on sustainability due to increased packaging and shipping demands.

4. Job displacement: Job displacement due to automation and ecommerce platforms, effects on working conditions, especially in logistics and delivery sectors.

5. Online safety and well-being: E-Commerce platforms may expose users to risks such as online scams, cyber bullying, and digital addiction. Ensuring online safety measures, providing digital literacy education, and promoting responsible digital citizenship are crucial for protecting the well-being of users, epically children and vulnerable populations.

Political Issues:

1. Regulatory Compliance:

   Developing and enforcing laws related to ecommerce transactions, data protection, and consumer rights, balancing regulation to foster innovation while ensuring ethical business practices.

2. Taxation: Addressing challenges related to collecting taxes on digital transactions and cross border ecommerce, ensuring fair taxation practices for online businesses operating globally.

3. Jurisdiction and Global Trade: Resolving conflicts related to jurisdiction in cross border transactions, impact of international trade agreements on ecommerce policies and regulations.

4. Data Sovereignty: Concerns over where data is stored and who has access to it, navigating international data protection laws and regulations.

5. Cyber security and National Security: E-Commerce platforms are vulnerable to cyber threats including data breaches, hacking attacks, and ransomware incidents.

6. Political influence and lobbying: E-Commerce companies engage in political lobbying and advocacy efforts to shape regulatory policies and influence legislative decision that impact their business interests.

A model for Organising ethical issues:

FIGURE 4.1 THE RELATIONSHIP BETWEEN ETHICAL, SOCIAL, AND POLITICAL ISSUES IN AN INFORMATION SOCIETY

The introduction of new information technology has a ripple effect, raising new ethical, social, and political issues that must be dealt with on the individual, social, and political levels. These issues have five moral dimensions: information rights and obligations, property rights and obligations, system quality, quality of life, and accountability and control.
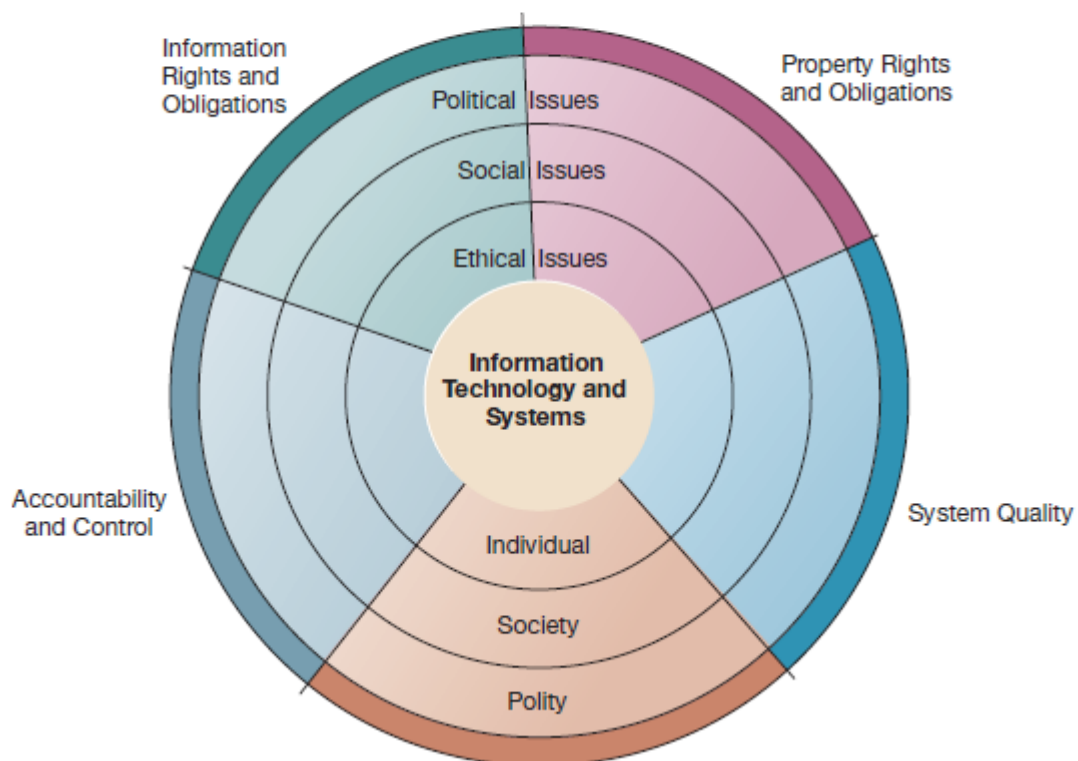
Organizing ethical issues involves structuring and addressing them in a systematic manner to ensure thorough consideration and appropriate decision making.

1. **Information rights and obligations:** This centres around the rights and obligations of individuals and organizations concerning the collection, use, and disclosure of information. This encompasses issues like data privacy, intellectual property rights, freedom of information, and responsible data governance.

2. **Political issues:** This brings to light the political ramifications of IT, such as the role of government in regulating its use, the impact of technology on democratic processes, and the potential for digital surveillance and censorship.

3. **Social Issues:** This delves into the social impacts of IT, including the digital divide, the influence of technology on privacy and security, the ethical considerations of artificial intelligence, and the potential for social division and exclusion.

4. **Quality of life:** this explores how IT can be harnessed to improve the quality of life for individuals and society as a whole. This encompasses areas like access to education and healthcare, the efficiency of public services, and the potential for technological advancements to address social challenges.

5. **Accountability and control:** This raises the crucial question of who is responsible for the ethical use of IT and how systems can be designed to be more accountable.

6. **Individual, society, Polity:** This underscores the diverse stakeholders impacted by IT, emphasizing the need to consider the interests of all groups when making decisions about technology. This includes individuals, communities, corporations, governments, and international organizations, whose perspectives and values should be integrated into responsible IT development and governance.

Information collected at E-Commerce websites:

Information collected at ecommerce websites typically includes a wide range of data points that are crucial for various purposes such as personalization,

marketing, transaction processing, and analytics. Here's an overview of the types of information commonly collected:

1. Personal Information:

Identification: Name, gender, date of birth, social security number (depending on region).

Contact Details: Address, email, phone number.

Payment Information: Credit card details, billing address, payment history.

2. Transactional Data:

Order History: Details of past purchases, including products bought, dates, and amounts spent.

Shopping Preferences: Items viewed, wish lists, shopping cart contents.

Shipping Information: Shipping address, preferred delivery options.

3. Behavioural Data:

Website Interactions: Pages visited, time spent on each page, clicks, searches performed.

Device Information: Type of device used (desktop, mobile), operating system, browser type.

Referral Sources: How the user arrived at the website (search engine, direct visit, referral link).

4. User generated Content:

Reviews and Ratings: Customer feedback on products and services.

Comments and Messages: Communications with customer service or other users on the platform.

5. Cookies and Tracking Technologies:

Cookies: Small text files stored on the user's device to track preferences and activities, tracking Pixels and Beacons: Used for analytics, advertising, and tracking user behaviour across websites.

6. Location Data:

IP Address: General location based on IP address.

GPS and Geo-location: More precise location data if permission is granted by the user.

7. Preferences and Settings:

Account Settings: User preferences, notifications settings.

Marketing preferences: Opt-ins or opt-outs for marketing communications.

<u>Purpose of Information Collection:</u>

Personalization: Customizing the user experience based on past behaviour and preferences.

Marketing and Advertising: Targeted ads and promotions based on user interests.

Transaction Processing: Facilitating payments and order fulfilment.

Analytics and Improvements: Understanding user behaviour to enhance website usability and performance.

Compliance and Security: Meeting legal and regulatory requirements, and ensuring data security.

Ethical and Privacy Considerations:

Consent: Ensuring users are informed and give consent for data collection and usage.

Security: Protecting collected data from unauthorized access, breaches, and misuse.

Transparency: Clearly communicating to users what data is collected and how it will be used.

Data Retention: Safely storing data and adhering to retention policies.

User Rights: Providing mechanisms for users to access, correct, or delete their personal data.

Legal protections Intellectual Property Rights:

Legal protections for intellectual property (IP) rights are crucial in ensuring creators and innovators have the necessary incentives and protections for their works and inventions. Here are the primary legal frameworks that protect **intellectual property rights:**

1. Copyright Law:

Purpose: Protects original works of authorship fixed in any tangible medium of expression (e.g., literary works, music, art, software).

Rights: Grants the creator exclusive rights to reproduce, distribute, perform, display, and create derivative works of their creation.

Duration: Generally lasts for the life of the author plus 70 years.

2. Patent Law:

Purpose: Protects inventions or discoveries that are novel, useful, and nonobvious.

Rights: Grants the inventor exclusive rights to prevent others from making, using, selling, or importing their invention for a limited period (usually 20 years).

Types: Utility patents (for processes, machines, articles of manufacture) and design patents (for ornamental designs of functional items).

3. Trademark Law:

Purpose: Protects words, phrases, symbols, or designs that distinguish goods or services in the marketplace.

Rights: Grants the owner exclusive rights to use the mark in commerce and to prevent others from using confusingly similar marks.

Duration: Can be renewed indefinitely as long as the mark is used and maintained properly.

4. Trade Secret Law:

Purpose: Protects confidential business information that provides a competitive advantage (e.g., formulas, processes, customer lists).

Rights: Protects against unauthorized use or disclosure as long as the information remains secret and efforts are made to keep it confidential.

Duration: Lasts indefinitely as long as the information remains secret.

International Treaties and Agreements:

WIPO (World Intellectual Property Organization): Administers international treaties such as the Berne Convention (copyright), the Paris Convention (industrial property), and the TRIPS Agreement (Trade Related Aspects of Intellectual Property Rights).

TRIPS Agreement: Sets minimum standards for intellectual property regulation within member countries of the World Trade Organization (WTO).

Enforcement and Remedies:

Civil Remedies: Lawsuits for injunctions, damages, and account of profits.

Criminal Enforcement: Penalties for wilful infringement, counterfeiting, or piracy.

Customs Enforcement: Seizure and detention of infringing goods at borders.

Ethical and Policy Considerations:

Balancing Rights: Ensuring IP laws balance incentives for innovation with public access and competition.

Access to Knowledge: Promoting access to essential knowledge and cultural goods while respecting IP rights.

Global Challenges: Addressing international harmonization, enforcement challenges, and evolving technologies (e.g., digital piracy, AIgenerated content).