1. Analyze the following statements regarding types of cybercrimes:  
I. Phishing often involves the attacker impersonating a trustworthy entity to solicit sensitive information.  
II. Identity theft includes unauthorized access and use of another person's payment card details.  
III. A DDoS (Distributed Denial of Service) attack primarily targets data theft from the victim's network.  
Which of the following is correct?  
(1) I and II only  
(2) I and III only  
(3) II and III only  
(4) All of the above  
Answer Key: 3  
Solution:  
• Statement I(Incorrect): While phishing does involve impersonation, it is typically to gain unauthorized access to systems or data, not just to solicit information.  
• Statement II(Correct): Identity theft encompasses various forms, including the unauthorized use of credit or debit card details, which is a common method.  
• Statement III(Correct): A DDoS attack aims to disrupt service by overwhelming the target with excessive requests, hence not for data theft but service disruption.  
Hence, Option (3) is the right answer.  
  
2. Consider the following statements about sousveillance as conceptualized by Steve Mann:  
I. Sousveillance is primarily a top-down monitoring process similar to surveillance.  
II. It involves the use of wearable computing devices to record and broadcast personal experiences.  
III. Sousveillance is considered a form of participatory monitoring where individuals engage in the collection and analysis of data about their environment.  
Which of the following is correct?  
(1) I and II only  
(2) I and III only  
(3) II and III only  
(4) All of the above  
Answer Key: 3  
Solution:  
• Statement I(Incorrect): Sousveillance, unlike surveillance, is a bottom-up approach, where individuals, not authorities, perform the monitoring.  
• Statement II(Correct): Steve Mann’s work heavily emphasizes the use of wearable technology to enable individuals to record interactions from their own perspective.  
• Statement III(Correct): It is indeed a participatory approach to monitoring, emphasizing personal empowerment and control over one’s own data.  
Hence, Option (3) is the right answer.  
  
3. Evaluate the following statements regarding Thomas Mathiesen's Synopticon and Michel Foucault's Panopticon:  
I. In the Panopticon model, visibility is a trap, where all inmates can be observed by a single watcher without them knowing if they are being watched.  
II. The Synopticon allows for the many to watch the few, which is a reversal of the Panopticon’s principle.  
III. Both Synopticon and Panopticon emphasize the power of secretive observation and control.  
Which of the following is correct?  
(1) I and II only  
(2) I and III only  
(3) II and III only  
(4) All of the above  
Answer Key: 1  
Solution:  
• Statement I(Correct): Foucault describes the Panopticon as a design where inmates are constantly visible to a central tower, without ever seeing the watcher, creating a sense of permanent visibility that serves as a control mechanism.  
• Statement II(Correct): Mathiesen's Synopticon describes a society where the many observe the few (e.g., media watching celebrities), which contrasts with Foucault’s concept where few observe the many.  
• Statement III(Incorrect): While the Panopticon involves secretive observation, the Synopticon involves more open and observable scrutiny, thus not primarily about secrecy.  
Hence, Option (1) is the right answer.  
  
1. In evaluating e-governance models, consider a scenario where a government portal is redesigned to enhance interactions primarily between government entities and citizens. The portal integrates services like tax filing, birth registration, and public grievance redressal. Reflecting on the redesign, which aspect would most likely not be a primary focus when optimizing for a G2C (Government to Citizen) model?  
(1) Enhancing inter-departmental data sharing mechanisms to streamline service delivery.  
(2) Integrating advanced cryptographic measures for secure online transactions.  
(3) Improving user interface and accessibility features to accommodate all citizen demographics.  
(4) Focusing on increasing backend process efficiencies between different government departments.  
Answer Key: 4  
Solution:  
• Option 4 (Incorrect): While backend process efficiencies are crucial for internal government operations (G2G), the primary focus in a G2C model should be on direct interactions and service delivery to citizens, not inter-departmental efficiency.  
• Option 1 (Correct): Enhanced data sharing between departments can directly improve the efficiency and effectiveness of citizen-facing services.  
• Option 2 (Correct): Security is paramount in citizen interactions to protect personal information and ensure trust in digital services.  
• Option 3 (Correct): Accessibility and user-friendly interfaces are essential in G2C models to ensure that all citizens can easily access and use government services.  
Hence, Option (4) is the right answer.  
  
2. Considering the application of algorithmic governance in law enforcement, specifically predictive policing, which statement most accurately reflects a potential limitation of this approach that could affect its effectiveness?  
(1) Predictive policing tools can help allocate resources more effectively by predicting crime hotspots based on historical data.  
(2) The use of advanced algorithms can remove human biases entirely from policing strategies.  
(3) Algorithmic models can update in real-time, incorporating the latest crime data to adjust predictions.  
(4) Reliance on historical crime data without considering socio-economic changes might perpetuate existing biases and lead to inequitable policing practices.  
Answer Key: 1  
Solution:  
• Option 1 (Incorrect): While predictive policing does aim to allocate resources efficiently, it does not inherently guarantee effective crime prevention or address the root causes of crime, which are critical for long-term effectiveness.  
• Option 2 (Incorrect): Algorithms often reflect the biases present in the data they are trained on, potentially leading to biased outputs rather than eliminating human biases.  
• Option 3 (Incorrect): Real-time updates are technically feasible but depend heavily on the infrastructure and data quality, which can vary significantly across different jurisdictions.  
• Option 4 (Correct): Historical data can indeed perpetuate existing biases if not critically analyzed and adjusted for socio-economic and demographic changes over time.  
Hence, Option (4) is the right answer.  
  
3. When assessing the pillars of Digital India, focusing on 'empowerment', which initiative would least likely contribute directly to empowering citizens through digital means?  
(1) Developing broadband highways to ensure high-speed internet access across rural and urban areas.  
(2) Creating platforms for electronic delivery of government services like e-Kranti.  
(3) Implementing comprehensive digital literacy programs to educate citizens about digital tools and resources.  
(4) Establishing a central repository for all academic awards to streamline data verification processes.  
Answer Key: 4  
Solution:  
• Option 4 (Incorrect): While a central repository for academic awards does contribute to the infrastructure and services pillars by enhancing data management and verification, it does not directly empower citizens in terms of digital access, skills, or participation in the digital economy.  
• Option 1 (Correct): Broadband highways are fundamental to ensuring that digital empowerment is possible by providing the necessary infrastructure for internet access.  
• Option 2 (Correct): Electronic delivery of services empowers citizens by making government services accessible and efficient.  
• Option 3 (Correct): Digital literacy drives are directly tied to empowering citizens by equipping them with the necessary skills to participate fully in the digital world.  
Hence, Option (4) is the right answer.  
  
1. In the context of the Banopticon theory, how does the application of risk profiling potentially lead to social exclusion in an urban setting where surveillance is implemented to reduce crime rates?  
(1) By fostering a culture of trust through transparent and accountable surveillance practices, mitigating any form of exclusion.  
(2) By disproportionately targeting marginalized communities based on predictive data, leading to increased scrutiny and potential isolation from societal benefits.  
(3) By enhancing community engagement and reducing crime through the deployment of equitable surveillance across all demographics.  
(4) By ensuring that all individuals are equally monitored, thereby eliminating any bias in surveillance practices.  
Answer Key: 2  
Solution:  
• Option 1 (Incorrect): Trust and accountability are positive outcomes, but they do not address the risk of profiling leading to exclusion.  
• Option 2 (Correct): Predictive policing based on profiling can disproportionately affect marginalized groups, leading to their exclusion from societal benefits and opportunities, aligning with the Banopticon concept.  
• Option 3 (Incorrect): While equitable surveillance could theoretically reduce crime, it does not specifically address how risk profiling leads to exclusion.  
• Option 4 (Incorrect): Equal monitoring is an ideal but does not consider the real-world application of predictive data which can lead to biased surveillance against certain groups.  
Hence, Option (2) is the right answer.  
  
2. How does the integration of public digital platforms like Aadhaar, UPI, and DigiLocker impact the socio-economic inclusion of rural populations in India?  
(1) By creating digital literacy programs that ensure all rural populations can equally benefit from these platforms.  
(2) By providing essential services and financial inclusion through seamless, secure, and accessible digital identities and transactions.  
(3) By increasing the digital divide due to the lack of necessary infrastructure and literacy in rural areas.  
(4) By solely improving urban infrastructures, thereby widening the gap between urban and rural technological access.  
Answer Key: 2  
Solution:  
• Option 1 (Incorrect): While digital literacy is crucial, the question focuses on the impact of platform integration, not the measures to enhance usability.  
• Option 2 (Correct): These platforms facilitate access to a variety of services like banking, government documents, and subsidies, directly enhancing socio-economic inclusion for rural populations.  
• Option 3 (Incorrect): This option points to a potential negative outcome, but the integration itself aims to bridge rather than widen the digital divide.  
• Option 4 (Incorrect): The question pertains to rural impacts, and this option diverts to urban improvement, which is not the focus.  
Hence, Option (2) is the right answer.  
  
3. Considering the principles of surveillance capitalism, what is the likely consequence of corporations harnessing personal data to predict and modify human behavior for profit maximization?  
(1) It fosters a mutually beneficial relationship between consumers and corporations by tailoring products to consumer needs.  
(2) It leads to enhanced security measures that protect consumer data from potential breaches and misuse.  
(3) It results in a loss of individual autonomy and privacy, as personal data is commodified without explicit consumer consent.  
(4) It promotes transparency in corporate practices, ensuring that consumers are fully aware of how their data is used.  
Answer Key: 3  
Solution:  
• Option 1 (Incorrect): While tailored products may seem beneficial, this doesn't address the core issue of autonomy and privacy erosion described in surveillance capitalism.  
• Option 2 (Incorrect): While important, this option does not deal with the consequences of behavior prediction and modification for profit.  
• Option 3 (Correct): This aligns with Zuboff’s surveillance capitalism theory, where personal data is mined and exploited to predict and modify behavior, often without the individuals' consent, leading to a significant loss of privacy and autonomy.  
• Option 4 (Incorrect): Transparency is often lacking in surveillance capitalism, contrary to what this option suggests.  
Hence, Option (3) is the right answer.  
  
23. In the context of e-KYC and Direct Benefit Transfer (DBT) workflows, which of the following statements are correct?  
I. e-KYC reduces the need for physical documents.  
II. DBT can only be implemented with Aadhaar linkage.  
III. e-KYC is solely based on biometric authentication.  
IV. DBT enhances transparency in fund distribution.  
Choose the correct answer from the options given below:  
(1) I and IV only  
(2) II and III only  
(3) I, II, and III only  
(4) All of the above  
Answer Key: 1  
Solution:  
Statement I (Correct): e-KYC simplifies verification processes by reducing dependency on physical documents.  
Statement II (Incorrect): DBT can be facilitated through various identifiers, not just Aadhaar.  
Statement III (Incorrect): e-KYC uses multiple modes of authentication including OTPs and biometrics.  
Statement IV (Correct): DBT directly transfers benefits into beneficiaries' accounts, increasing transparency.  
Hence, the correct answer is Option (1).  
  
24. Regarding smart-city surveillance, which of the following statements are correct?  
I. CCTV reduces crime rates.  
II. IoT devices are infallible in data collection.  
III. ANPR systems can track vehicle movements.  
IV. Surveillance raises privacy concerns.  
Choose the correct answer from the options given below:  
(1) I and IV only  
(2) II only  
(3) III and IV only  
(4) I, II, and III only  
Answer Key: 3  
Solution:  
Statement I (Incorrect): While CCTV is intended to deter crime, its effectiveness in reducing crime rates is debatable and varies.  
Statement II (Incorrect): IoT devices can be prone to errors and vulnerabilities, affecting data accuracy.  
Statement III (Correct): ANPR systems are specifically designed to read and record vehicle number plates.  
Statement IV (Correct): Increased surveillance often leads to raised privacy and civil liberty concerns.  
Hence, the correct answer is Option (3).  
  
25. Which of the following statements are correct regarding online harassment issues such as cyberstalking and cyberbullying?  
I. Cyberstalking involves repeated harassment.  
II. Cyberbullying cannot be anonymous.  
III. Doxxing is the publication of private information.  
IV. Revenge porn is a form of cyberbullying.  
Choose the correct answer from the options given below:  
(1) I and II only  
(2) II and III only  
(3) I, III, and IV only  
(4) All of the above  
Answer Key: 3  
Solution:  
Statement I (Correct): Cyberstalking is characterized by persistent and repeated online harassment, making it a serious issue.  
Statement II (Incorrect): Cyberbullying often occurs anonymously, complicating prevention and response.  
Statement III (Correct): Doxxing specifically involves the unauthorized release and publication of private or identifying information.  
Statement IV (Correct): Revenge porn is recognized as a form of cyberbullying, exploiting private media to harm individuals.  
Hence, the correct answer is Option (3).  
  
1. Consider the following scenarios related to Sections 66C, 66D, 67, and 67A of the IT Act 2000/2008:  
I. A person creates a fake email account using another individual's personal information and uses it to solicit funds from the public.  
II. An individual digitally alters explicit images of a person without consent and disseminates them on social media platforms.  
III. Using a fraudulent digital identity, someone impersonates a government official to secure sensitive information from citizens.  
IV. A company inadvertently leaks user data due to insufficient security measures, leading to unauthorized access to personal information.  
V. An individual sends emails containing obscene content using their own legally registered email address.  
Choose the correct answer from the options given below:  
(1) I, II, and III only  
(2) II, III, and IV only  
(3) I, III, IV, and V only  
(4) I, II, and III only  
Answer Key: 4  
Solution:  
• Statement I(Correct): This scenario directly relates to Section 66D, which deals with cheating by personation using computer resources. Creating a fake email for soliciting funds fits this violation.  
• Statement II(Correct): This falls under Section 67A, which penalizes the electronic publication or transmission of material containing sexually explicit acts or conduct in electronic form without consent.  
• Statement III(Correct): Again, this pertains to Section 66D of the IT Act, which covers the offense of personation using electronic means, particularly when done to deceive or harm others.  
• Statement IV(Incorrect): This situation might involve a breach of reasonable security practices under Section 43A of the IT Act, which is not listed among the sections we are focusing on (66C, 66D, 67, 67A).  
• Statement V(Incorrect): While distasteful, sending obscene content using one's own email does not fall under the specified sections if not involving deceit or explicit material as defined under Section 67 or 67A.  
Hence, Option (4) is the right answer.  
  
2. Consider these practices in the context of data anonymization, pseudonymization, and de-identification:  
I. Removal of all direct identifiers from a dataset, ensuring no specific individual can be identified.  
II. Process of replacing personal identifiers in a dataset with artificial identifiers or pseudonyms.  
III. Data manipulation where original data values are replaced with values that preserve statistical distributions but are unrelated to the true values.  
IV. A method where data is encrypted using a key, which the processor retains, allowing for potential re-identification.  
V. Application of a statistical method to blur data, such as adding random noise to each data point in a set.  
Choose the correct answer from the options given below:  
(1) I, III, and V only  
(2) II, IV, and V only  
(3) I, II, and IV only  
(4) I, II, and V only  
Answer Key: 1  
Solution:  
• Statement I(Correct): This describes a de-identification technique where direct identifiers are removed to prevent the identification of individuals, adhering to privacy laws and guidelines.  
• Statement III(Correct): This refers to data masking or synthetic data generation, a form of anonymization where true values are replaced but statistical integrity is maintained.  
• Statement V(Correct): Adding random noise is a method of differential privacy, a technique used in anonymization to enhance privacy while preserving the utility of the data.  
• Statement II(Incorrect): Replacing identifiers with pseudonyms defines pseudonymization, not anonymization; the data can still potentially be re-identified if additional information becomes available.  
• Statement IV(Incorrect): Encryption with retained keys is a form of pseudonymization; the data remains reversible and does not achieve full anonymization.  
Hence, Option (1) is the right answer.  
  
3. Analyze the implications of Foucault’s concept of the Panopticon and disciplinary power in the following contexts:  
I. A corporation uses extensive surveillance to monitor employee productivity and enforce corporate policies.  
II. A government employs city-wide CCTV surveillance to deter criminal activities and enforce law.  
III. An online platform uses algorithms to monitor user behavior and personalize content delivery.  
IV. A teacher uses a point system where students' behavior is constantly monitored and rewarded.  
V. A social media company analyzes user data to predict and influence purchasing behaviors.  
Choose the correct answer from the options given below:  
(1) I, II, and IV only  
(2) I, III, IV, and V only  
(3) II, III, and IV only  
(4) II, IV, and V only  
Answer Key: 1  
Solution:  
• Statement I(Correct): This scenario closely aligns with Foucault's Panopticon, where surveillance is used as a tool of power and control within a disciplinary institution, in this case, a corporation.  
• Statement II(Correct): The use of CCTV by governments as a means of societal control and deterrence through constant surveillance also reflects the principles of the Panopticon.  
• Statement IV(Correct): The educational use of a point system for behavior monitoring and rewards mimics the Panopticon’s concept of continuous observation linked to disciplinary power, shaping and controlling behavior.  
• Statement III(Incorrect): While online platforms monitor user behavior, the primary intent here is content personalization rather than disciplinary power or social control, thus slightly diverging from Foucault’s original concept of the Panopticon.  
• Statement V(Incorrect): Analyzing user data for predicting purchasing behaviors involves manipulation and economic exploitation more than disciplinary power in its traditional Foucauldian sense.  
Hence, Option (1) is the right answer.