Teacher Answer Key

Case Study

1. Carlos assumed his conversations were private, but the reading notes that mental health apps frequently share data with third parties including advertisers and data brokers. His disclosed information — anxiety, intrusive thoughts, immigration concerns — is exactly the kind of sensitive personal data that AI systems can use to make inferences that he would never want shared. Additionally, the app may use conversation data to train its AI, and the conversational format creates a false sense of confidentiality that may not reflect the reality of data use.

2. The concept that applies is the mosaic effect — individually innocuous data points assembled into a comprehensive profile reveal far more than any single piece. If the app shares "anonymized" data that includes age, ZIP code, mood logs, and written content, combining those elements may allow re-identification of Carlos specifically, since the combination is unique enough to distinguish him from others in the dataset.

Multiple Choice

1. B
2. A
3. C

Matching

1-E, 2-D, 3-B, 4-A, 5-C

Fill-in-the-Blank

1) mental, 2) 13, 3) innocuous

Short Answer (Sample Responses)

Q1: AI systems can make inferences from data that the individual considers harmless — inferring health conditions from search histories, political beliefs from social media activity, sexual orientation from purchasing patterns. This means that no data is truly innocuous when AI can process it, and that comprehensive profiles can be assembled from information the person never thought of as sensitive. The mosaic effect means the combination is far more revealing than any individual piece.

Q2: Data brokers are companies that collect personal information from many sources — apps, retail programs, public records, social media — and sell comprehensive profiles to paying customers. The reading identifies them as largely unregulated in the U.S., which means the data they compile and sell can be used in

ways that harm individuals, including being used to identify, surveil, or discriminate against them in contexts completely unrelated to the original data collection.

Q3: The reading argues that meaningful protection requires limits on what data can be collected in the first place, restrictions on how it can be used, and enforcement with consequences proportionate to the harm. Disclosure requirements — like privacy policies — fail because most users do not read them and would not understand the full implications if they did. The underlying problem is collection and use, not just awareness, so protection must intervene at those earlier stages.