

## Instructions

There are **85 total points**. When asked to provide your answer within a figure or table, be careful to not exceed box boundaries. Bubbles must be filled out completely: ● is correct, ☑ ● ✕ are incorrect. All answers must be given within the provided circles, answer boxes, figures or tables. Write your full name in the box to acknowledge the instructions.

## Privacy Law and Regulation

**1. [4 points]:** According to the Fair Information Practice Principles (FIPPs) from the 1973 HEW report, which of the following are among the five core principles? (Select all that apply.)

- ☐ No secret record-keeping by organizations
- ☐ Right to know what data is collected and how it's used
- ☐ Prevention of secondary use without explicit consent
- ☐ Mandatory encryption of all personal data
- ☐ Requirement for reasonable security precautions

**2. [3 points]:** What is a significant limitation of the FIPPs model when applied to modern data systems?

- ☐ FIPPs require too much computational power to implement
- ☐ FIPPs assume static databases and don't address queries, machine learning, and probabilistic inference
- ☐ FIPPs only apply to government databases, not private companies
- ☐ FIPPs mandate opt-in consent, which is too restrictive for modern services

**3. [4 points]:** Which of the following are characteristics of the US privacy law approach? (Select all that apply.)

- ☐ Sectoral approach with laws specific to data holder types
- ☐ No comprehensive federal privacy statute
- ☐ Single omnibus privacy law covering all sectors
- ☐ FTC acting as de facto privacy regulator through Section 5 of the FTC Act
- ☐ State-level breach notification laws in all 50 states

**4. [3 points]:** Explain why the notice and consent model has been criticized as insufficient for protecting user privacy in practice.

(Answer inside the box)

Initials: \_\_\_\_

## GDPR and International Privacy

**5. [3 points]:** Some critics argue that GDPR's complexity and compliance costs create competitive advantages for large incumbent companies like Google and Facebook. Explain one reason why GDPR might strengthen the market position of these incumbents.

(Answer inside the box)

**6. [4 points]:** Which of the following are key requirements or provisions of GDPR? (Select all that apply.)

- ☐ Companies can collect any data as long as they notify users
- ☐ Consent must be opt-in only, not opt-out
- ☐ Right to be forgotten (data erasure)
- ☐ Maximum fine of \$1 million for violations
- ☐ Restrictions on cross-border data transfers

## CCPA/CPRA and Automated Compliance

**Example:** A website's opt-out page requires users to complete a multi-step process: first filling out a form with their full name, email address, phone number, and mailing address, then completing a CAPTCHA, and finally waiting for an email confirmation link that expires in 24 hours. The website claims this is needed to "verify identity and process the request."

**7. [4 points]:** What type of dark pattern does this example primarily represent?

- ☐ Confirm shaming
- ☐ Obstruction
- ☐ Misdirection
- ☐ Nagging

**8. [2 points]:** What is the Global Privacy Control (GPC) and how does it relate to CPRA compliance?

(Answer inside the box)

Initials: \_\_\_\_

**9. [3 points]:** Explain what the "spillover effect" (or "California effect") refers to in the context of privacy regulation compliance.

(Answer inside the box)

**10. [4 points]:** Studies of CCPA/CPRA compliance found that approximately 30% of covered entities failed to implement an opt-out link or mechanism on their website. Which of the following are valid reasons for this? (Select all that apply.)

- ☐ The sites don't actually sell data, so no opt-out link is required
- ☐ Implementation errors where links are hidden by JavaScript
- ☐ Opt-out functionality is in the privacy policy but not in a visible header/footer link
- ☐ All covered entities intentionally violate the law
- ☐ Links are dynamically loaded and absent from HTML source

## Dark Patterns

**11. [3 points]:** Explain why CPRA (California Privacy Rights Act) explicitly prohibits the use of dark patterns in the opt-out process.

(Answer inside the box)

**12. [4 points]:** Which of the following are examples of the "obstruction" category of dark patterns? (Select all that apply.)

- ☐ Requiring CAPTCHA completion to access privacy portal
- ☐ Mutually exclusive choices like "opt out of sale OR sharing, but not both"
- ☐ Asymmetry where opting in takes 1 click but opting out takes 2 clicks
- ☐ Using confusing language like "Allow sale" on an opt-out button
- ☐ Identity verification that fails if not completed within 48 hours

**Case Study:** A website's privacy opt-out page displays a toggle switch with no text labels. The switch is currently in the "off" position. Above the switch, text reads "Manage your privacy preferences." It's unclear whether toggling the switch to "on" will enable data selling or enable privacy protection. At the bottom of the page, there is a hyperlink labeled "this form" that is difficult to identify as clickable because it appears in the same color as regular text.

**Initials:** \_\_\_\_

**13. [2 points]:** Identify which category (or categories) of dark patterns are present in this case study and explain your reasoning.

(Answer inside the box)

**14. [3 points]:** Explain why the use of OneTrust or similar third-party compliance services does not guarantee actual compliance with privacy regulations.

(Answer inside the box)

## AI and Privacy

**15. [4 points]:** Which of the following represent AI-specific privacy risks that **differ from traditional** privacy risks? (Select all that apply.)

- ☐ Model memorization of training data
- ☐ Human-like interactions encouraging progressive disclosure
- ☐ Data breaches and unauthorized access
- ☐ Prompt injection attacks extracting sensitive information
- ☐ Use or sale of data to third parties

**16. [3 points]:** What is the "interdependent privacy" problem in the context of LLM usage?

- ☐ LLMs require multiple users to verify their identities
- ☐ Privacy settings must be configured by both the user and the LLM provider
- ☐ Users' privacy decisions affect others when they share information about colleagues, clients, or family
- ☐ LLMs cannot function without sharing data across multiple servers

**17. [3 points]:** Explain how anthropomorphization of LLMs can lead to increased privacy risks for users.

(Answer inside the box)

Initials: \_\_\_\_

**Scenario:** An LLM interface displays a prompt: "Do you want me to remember our chats to provide better context and more personalized responses in future conversations?" with buttons for "Yes, remember" and "No, don't remember."

**18. [4 points]:** Analyze this interface design for potential dark patterns. Does it exhibit characteristics of obstruction, interface interference, or misdirection? Explain your answer.

(Answer inside the box)

**19. [4 points]:** Which of the following are strategies users employ to protect privacy when using LLMs? (Select all that apply.)

- ☐ Accepting risks as a privacy-convenience tradeoff similar to other tech services
- ☐ Avoiding certain uses like financial data with real numbers
- ☐ Rewriting prompts to reduce identifiable information about gender, race, or location
- ☐ Only using LLMs through VPNs to hide IP addresses
- ☐ Not using LLMs for work-related queries due to company policies

## Copyright and Fair Use

**20. [4 points]:** Which of the following can be protected by copyright? (Select all that apply.)

- ☐ Mathematical formulas
- ☐ Literary works
- ☐ Ideas and concepts
- ☐ Software code
- ☐ Historical facts

**21. [4 points]:** By default, copyright grants the creator exclusive rights including making copies, distributing works, creating derivatives, and public performance. ☐ Yes ☐ No

**22. [4 points]:** According to fair use doctrine, which of the following are among the four factors courts consider when determining whether use of copyrighted material qualifies as fair use? (Select all that apply.)

- ☐ Whether the user obtained permission from the copyright holder
- ☐ Purpose and character of use (transformative use)
- ☐ Nature of the copyrighted work
- ☐ Amount and substantiality of portion used
- ☐ Effect on market value of the original work

**Initials:** \_\_\_\_\_

**Case Study:** An AI company trains a large language model (LLM) using millions of copyrighted books, articles, and creative works without obtaining permission from or compensating the authors. The company argues that this constitutes fair use. Authors have filed lawsuits claiming copyright infringement, arguing that AI-generated content competes with their work and threatens their livelihoods. The case is expected to reach the Supreme Court.

- 23. [3 points]:** Using the "transformative use" test from fair use doctrine, construct an argument IN FAVOR of the AI company's fair use defense.

(Answer inside the box)

- 24. [3 points]:** Using the "effect on market value" test from fair use doctrine, construct an argument AGAINST the AI company's fair use defense.

(Answer inside the box)

## Feedback

- 25. [1 point]:** Interest (1=Boring!; 10=Amazing!):

Difficulty (1=Too easy; 10=Too hard):

- 26. [2 points]:** 1. One topic you found most interesting this semester. 2. One suggestion for improvement:

(Answer inside the box)

**Initials:** \_\_\_\_