5.3 Security and Privacy
By Mary Kane

Answers 5.3 Data Ethics

In this task, you'll identify and respond to potential data security and privacy issues at Pig E. Bank.

Step 1: Read the following scenario and answer the questions

Your role at Pig E. Bank is to develop models that detect suspicious account activity associated with money laundering. Your current project requires you to distribute prototype model outputs to your team of investigators for validation. Standard investigation procedure requires the investigator to access client PII and account information to build a customer profile before dispositioning the model output. One day, you notice one of your investigators taking a photo of his screen while sensitive client data is displayed.

1) Is this a data privacy issue, a data security issue, or both? Both.

- Data security: Taking a photo of a screen with PII is an unauthorized way of copying and removing sensitive data from a controlled system (possible exfiltration).
- Data privacy: The photo contains client PII, so it risks improper use or disclosure of personal information.

2) Risks to Pig E. Bank and its customers if not addressed

- Customer harm: identity theft, fraud, account takeover, stalking/harassment if addresses or other details are exposed.
- Bank harm: regulatory violations (privacy/GLBA-type obligations), fines, lawsuits, mandatory breach notifications, reputational damage, loss of customer trust.
- Operational harm: compromised investigations, insider threat expansion (others may copy data), increased monitoring and remediation costs.

3) Policy changes to prevent this type of data theft (data access + controls)

Access & handling rules

- Explicit policy: no photography/screenshots of customer data, no copying to personal devices, no external storage.
- Require annual training + signed acknowledgment for investigators handling PII.

5.3 Security and Privacy
By Mary Kane

Technical controls

- Use a secure investigation environment (VDI) with:
    - Disable screenshots/clipboard/printing/USB
    - Watermark screens with user ID + timestamp (deters and helps investigate leaks)
    - Session recording for high-risk queues
- Least privilege access: investigators see only the PII fields needed; hide sensitive fields by default ("view more" with logging).

Monitoring & enforcement

- Strong insider-threat monitoring: logs for unusual access, bulk lookups, after-hours activity.
- Clear escalation: immediate report, investigation, and consequences (up to termination).

5.3 Security and Privacy
By Mary Kane

Step 2: Read the following scenario and answer the questions

Your manager has asked you to join them in representing the compliance analytics department at the compliance committee meeting. At the meeting, the prospect of outsourcing some lower-level analytical functions to a contractor in a foreign country is discussed, and it is popular with the other department heads. Outsourcing could save the bank millions of dollars annually in labor costs, and the department heads seem confident that this won't violate data privacy laws. You know from experience that some of your bank's customers can be identified as being on active military duty, and, like all clients, you keep records of their pay grade, address, contact information, and other PII.

1) **Does this scenario highlight a data privacy issue, a data security issue, or some other ethical issue?**

This scenario raises both data privacy and data security issues, as well as an ethical risk.

Data privacy issue: Outsourcing analytics to a contractor in another country likely involves cross-border access to and transfer of customer PII (addresses, contact info, payment details).

That can trigger different security issues involving privacy laws and restrictions on international data sharing, contractual limits on how customer data can be used, stored, and retained, and major privacy risks and ethical concerns regarding customers with sensitive data (active-duty military).

2) **How would you communicate your concerns to the compliance committee? Be as specific as you can.**

a. The goal: I understand the cost savings, and I am open to outsourcing lower-level work, but we need to confirm we are not creating a privacy or security incident.

b. Key risk: The fact that we are giving access to PII data to a cross-border third party changes our legal and control requirements.

c. Sensitive group: Some customers can be identified as active-duty military, if their PII data is mishandled, the harm and reputational impact could be much higher.

d. The Plan: I propose we approve outsourcing after confirming:

- Privacy and legal transfer rules for the cross-border third party.
- Security controls to use (enforce no downloads or screenshots, session logging, role-based access, watermarking)
- We complete a PIA (Privacy Control Assessment)

- A pilot proves controls work (monitored outcomes)

"Outsourcing may save money, but this is cross-border third-party handling of customer PII, including data that can identify active-duty military customers. That increases privacy, security, and reputational risk. I recommend we pause approval until we complete a formal privacy/legal and third-party security review, and design the workflow so contractors only access the minimum data inside a bank-controlled secure environment with logging and no-download controls."

3) **If Pig E. Bank does go ahead and outsource some of its analytical functions, how would you anonymize the data while ensuring that someone can still conduct an analysis? (Use the information and resources provided in the Exercise to answer this question; there's no need to go into technical details.)**

Minimize data providing only necessary data (Account age, time between deposit/withdraw, deposit/withdrawal amounts rounded up, daily or weekly frequency, broad location US or MX). Mask direct Identifiers, replacing any needed ID with tokens.

Limit sensitive attributes, or generalize the occupation category if needed (government, health, service, education)

Step 3: Read the following scenario and answer the questions

Suppose you've lived and worked in different cities around the world, and you're interested in learning more about how other countries have dealt with data ethics.

- Research a case study from your country where a company or organization has unethically collected and shared data. You're free to use information you find online, but make sure you include the link to your resources in your document.
- Explain what the company or organization did. Did they act according to regional or national laws?
- Why was the company's behavior unethical? (To answer this question, refer to this Exercise and the previous Exercise on data bias.)
- What could the company have done to prevent this unethical behavior? Please provide some concrete suggestions.

5.3 Security and Privacy
By Mary Kane

Case study (United States): Alleged improper sharing of Social Security data tied to "DOGE"

A. What the organization did

Multiple reports describe a whistleblower complaint and court filings alleging that staff connected to the "Department of Government Efficiency" ("DOGE") moved or shared Social Security Administration (SSA) data outside approved SSA environments, including use of a third-party cloud service (Cloudflare) that SSA said was not approved for storing SSA data.

A whistleblower disclosure (reported by ABC News) alleged that a copy of extremely sensitive SSA records—potentially including Social Security numbers and other PII—was placed in a "vulnerable cloud environment," creating major exposure risk if accessed by unauthorized parties; SSA responded publicly that it stores personal data in secure environments and said it was not aware of a compromise.

B. Did they act according to national laws?

Based on public reporting, legality is disputed and/or under investigation, but there are strong signs of serious violations of privacy and security obligations-

Potential noncompliance:

- **Privacy Act of 1974:** The Privacy Act restricts disclosure of records about individuals from a federal "system of records" without consent unless a statutory exception applies.
- **Court/lawsuit context**: Reuters reported a federal judge blocked SSA from further data sharing with DOGE, saying SSA likely violated privacy laws (as described in the ruling).
- **Hatch Act referrals**: DOJ court filings described referrals related to possible Hatch Act issues (political activity restrictions for federal employees), which is a separate—but related—governance/ethics signal.

C. Why the behavior was unethical (privacy + bias lens)

- Even if someone argued "we were trying to reduce fraud," the alleged actions are ethically problematic because they conflict with core privacy and responsible data principles:
- **Purpose limitation/misuse risk:** SSA data is collected for administering Social Security programs. Moving or sharing it outside approved workflows increases the chance it's used for purposes the public didn't agree to (or even know about).

5.3 Security and Privacy
By Mary Kane

- **Data minimization failure:** Uploading or exposing broad, population-scale datasets (millions of records) is ethically excessive if the task only requires limited fields or aggregated features. Bigger datasets = bigger harm when something goes wrong.
- **Lack of transparency and oversight:** The reporting emphasizes SSA allegedly didn't have clear visibility/control over what was shared and where it lived (e.g., inability to track access). That violates the ethical duty to steward sensitive data carefully.
- **Risk of disproportionate harm (bias connection)**
  When sensitive government datasets are accessed or repurposed, the negative impact often falls hardest on vulnerable groups (e.g., people who rely on benefits, people exposed to identity theft). In biased terms, even "neutral" data actions can create unequal harm if certain groups are more exposed or more likely to be targeted by downstream use.

2 DOGE staffers at Social Security agency may have violated Hatch Act, DOJ says

Whistleblower complaint alleges DOGE uploaded all Social Security numbers to an unsecured server - ABC News

Yes, 'DOGE' did put our Social Security data at risk. Here's what lawmakers are doing about it. | Congressman John Larson