Step 1

1. **Is this a data privacy issue, a data security issue, or both? Please provide a short explanation for your answer.**
   This is **both a data privacy and data security issue**.

- **Data Privacy Issue**: Taking a photo of the screen displaying personally identifiable information (PII) violates policies designed to protect sensitive client data. It risks exposing customers' private information to unauthorized parties and breaches privacy regulations like GDPR or CCPA.
- **Data Security Issue**: Photographing sensitive information circumvents established security controls (e.g., access logs, encryption, or screen monitoring). The data could be shared, stored on insecure devices, or used in unauthorized ways, leading to potential breaches.
  Both privacy and security are compromised because the act exposes sensitive data beyond the intended environment, without any monitoring or approval.

2. **What would be the risks to Pig E. Bank and its customers if this issue weren't addressed?**

If the issue of unauthorized photographing of sensitive data isn't addressed, Pig E. Bank and its customers could face several significant risks:

1. Legal and Regulatory Risks

- **Regulatory Fines**: Violations of privacy laws like GDPR, CCPA, or GLBA can lead to steep fines.
- **Lawsuits**: Affected customers may file class-action lawsuits if their data is mishandled or leaked.

2. Financial Risks

- **Compensation Costs**: The bank may have to offer financial compensation, such as refunds or identity theft protection.
- **Operational Costs**: Handling investigations, audits, or remediation after a breach can be costly and disruptive.

3. Reputational Damage

- **Loss of Customer Trust**: Customers may leave if they feel their personal information isn't protected.
- **Negative Publicity**: News of poor data handling practices could damage the bank's brand, making it harder to attract new clients.

4. Customer Risks

- **Identity Theft and Fraud**: Exposed PII can be used to create fraudulent accounts or access existing ones.

- **Targeted Scams**: Criminals may exploit leaked data to launch phishing attacks or other scams against customers.

5. Operational Risks

- **Internal Policy Violations**: Allowing such behavior creates a culture of non-compliance, weakening internal security practices.
- **Increased Audit and Oversight**: Regulators may impose additional audits and monitoring, increasing administrative burdens.

In summary, failing to address this issue could have severe consequences for the bank's finances, operations, legal standing, and customer trust.

3. To prevent this type of data theft in the future, what changes would need to be made to the policies around data access?

1. Strengthen Data Access Policies

- Prohibit Personal Device Usage: Explicitly forbid the use of personal devices (like phones or cameras) in areas where sensitive data is accessed.
- Clear Screen Policy: Implement rules requiring screens to be locked when not in use and minimize displaying unnecessary PII.
- Role-Based Access Control (RBAC): Limit data access to only the information investigators need to perform their tasks (principle of least privilege).

2. Implement Monitoring and Auditing Procedures

- Screen Recording and Monitoring: Use tools to monitor screen activity or detect abnormal usage patterns (e.g., screenshots or long viewing periods).
- Regular Audits: Schedule periodic audits of user access logs and actions to detect and deter unauthorized behavior.

3. Increase Physical and Technical Security Controls

- Restricted Areas: Limit access to spaces where sensitive data is viewed to authorized personnel only, and enforce security checks (e.g., badge scans, CCTV).
- Device Management: Provide approved work-only devices to investigators and use software to disable unauthorized screenshots or screen captures.
- Watermarking: Apply dynamic watermarks on screens to discourage photography and make photos traceable to specific users.

4. Awareness and Training Programs

- Training on Data Security: Provide regular training to all employees on data handling policies and the consequences of non-compliance.
- Incident Reporting Process: Ensure employees know how to report suspicious behavior or policy violations confidentially.

5. Legal and Disciplinary Frameworks

- Revise Acceptable Use Policies: Add explicit language prohibiting photographing or copying sensitive data without authorization.
- Zero-Tolerance Policy: Enforce clear disciplinary actions (e.g., suspension or termination) for violations, and communicate these consequences to employees.

6. Leverage Technology Controls

- Screen Capture Detection Software: Use tools that can block or log any attempt to take screenshots or screen recordings.
- Virtual Desktop Infrastructure (VDI): Implement VDI so sensitive information is displayed only in controlled environments, with restricted export options.

These measures will create a **comprehensive approach** to secure data access, deter data theft, and ensure employees adhere to privacy and security policies.

Step 2

1. Does this scenario highlight a data privacy issue, data security issue, or some other ethical issue? Explain your answer.

1. Data Privacy Issue

- Cross-Border Data Transfer Risks: Sharing sensitive customer information, such as PII and military status, with a contractor in a foreign country could violate data privacy laws, depending on the location and regulatory frameworks. Regulations like GDPR, CCPA, or GLBA may impose restrictions on sharing PII with third parties, especially across national borders.
- Special Protections for Military Personnel: Military personnel data, especially in active service, may be subject to additional privacy protections under specific regulations (e.g., the Servicemembers Civil Relief Act (SCRA) in the U.S.). Mishandling such data could put these individuals at personal and operational risk.

2. Data Security Issue

- Third-Party Security Risk: Outsourcing introduces new risks, such as unauthorized access, insecure systems, and improper handling of data by the contractor. You need to ensure that the contractor has strong data security practices in place, equivalent to your bank's standards.

- Vendor Management Challenges: Once data is transferred, it becomes harder to control who accesses it and how it’s used, raising the risk of insider threats or data breaches.

3. Ethical Concerns

- Trust and Transparency with Clients: Outsourcing sensitive data processing may erode customer trust, especially if customers are not informed or do not consent to this arrangement.
- Risk to Military Clients: Exposing the PII of military personnel could compromise their safety (e.g., targeted phishing attacks or identity theft), which carries national security implications beyond financial risks.
- Due Diligence and Accountability: There is an ethical obligation to ensure that contractors in foreign countries handle sensitive data responsibly, with the same care as the bank would, which may not always be guaranteed.

2. **How would you communicate your concerns to the compliance committee? To answer this question, you can rely on either your previous work experience or the tips provided in the Exercise but be as specific as you can.**

When communicating concerns to the compliance committee, it’s essential to be clear, concise, and solutions oriented. Here's a structured approach I would use:

1. Prepare with Facts and Regulations

- Research relevant **laws** (e.g., GDPR, CCPA, GLBA, SCRA) and identify how they apply to outsourcing PII, especially for military personnel.
- Gather examples of outsourcing failures or risks (e.g., breaches, regulatory fines) to illustrate potential consequences.

2. Use a Structured Communication Framework (What, Why, Impact, Solution)

A. Start with the Issue ("What")

- "I’d like to highlight a potential concern with outsourcing certain analytics functions to a foreign contractor. Specifically, the data we’d be sharing includes sensitive PII, and some of this pertains to customers on active military duty."

B. Explain the Importance ("Why")

- "Because this data contains military status, pay grades, and contact information, it’s subject to additional privacy regulations and protections. Mishandling this data could expose our bank to regulatory non-compliance risks under laws like the SCRA, GLBA, or GDPR if the contractor operates in a jurisdiction without equivalent data privacy standards."

C. Describe the Impact if Unaddressed ("What Happens if We Ignore This?")

- "If the data isn't properly secured or is accessed by unauthorized individuals, there could be serious consequences, including:
  - Reputational harm if military personnel or other customers lose trust in the bank.
  - Legal and regulatory fines for cross-border data violations.
  - Operational risks if the military PII is compromised, leading to fraud, phishing attacks, or national security concerns."

D. Offer Solutions ("How We Can Address It")

- "To mitigate these risks, I recommend the following steps:
  1. Vendor Due Diligence: Assess the contractor's security practices and ensure they meet our data protection standards.
  2. Legal Review: Confirm whether sharing data across borders complies with privacy laws and determine if customer consent is required.
  3. Data Minimization: Limit the amount of sensitive data shared with the contractor.
  4. Auditing and Monitoring: Implement regular audits to monitor how the contractor handles our data."

3. Invite Discussion and Collaboration

- "I understand that outsourcing offers significant cost savings, and I am fully supportive of finding efficient solutions. I just want to ensure that we pursue this initiative safely and in compliance with all relevant laws. I'd be happy to work with the legal and vendor management teams to address these concerns."

4. Use a Professional and Constructive Tone

Throughout the conversation, I would emphasize that my goal is to protect the bank and its customers while supporting the committee's objectives. This way, the discussion stays collaborative rather than confrontational.

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.)**

1. Data Masking (Hiding Identifiable Information)

- Replace names, phone numbers, and addresses with fictional or randomized values.
- Use tokenization to swap sensitive fields (e.g., customer ID) with random tokens that have no meaning outside the analysis environment.

2. Data Aggregation (Grouping Data)

- Group individual records into summary statistics (e.g., averages, totals, or percentiles). For example, instead of analyzing specific pay grades, analyze average salaries by role or region.
- This reduces the risk of identifying individual customers while retaining analytical value.

3. Pseudonymization (Linking Data Safely)

- Replace personally identifiable information (PII) with pseudonyms (e.g., assigning a random customer ID) while keeping the mapping key secured.
- This ensures that individual records can be linked across datasets, if necessary, but without directly identifying anyone.

4. Generalization (Broadening Data Categories)

- Broaden specific data points to less granular levels. For instance:
  - Use age ranges (e.g., 20–30) instead of exact birth dates.
  - Replace specific addresses with ZIP codes or regions.

5. Differential Privacy (Adding Noise)

- Introduce random noise to datasets to make it difficult to identify individuals. For example, slightly modify numerical data (e.g., incomes) while ensuring the analysis remains valid for trends and averages.

6. Data Minimization (Remove Unnecessary Data)

- Limit the outsourced data to only the fields essential for the contractor's work. For instance, omit contact information or military status if it's not needed for the specific analysis.

7. Synthetic Data (Creating Artificial Data)

- Generate synthetic datasets that mimic the statistical properties of real data without exposing any actual customer information.

Step 3

1. **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.**

A well-known example of unethical data collection is the *Facebook-Cambridge Analytica* scandal, which became public in 2018. In this case, Cambridge Analytica, a political consulting firm, harvested data from millions of Facebook users without their explicit consent. This data was collected through a third-party app called "This Is Your Digital Life," which asked users to participate in personality quizzes. However, the app not only accessed the quiz-takers' data but also that of their Facebook friends, ultimately compiling information on approximately 87 million users.

This harvested data was used to build psychological profiles for targeted political campaigns, influencing voters in events such as the 2016 U.S. Presidential election and the Brexit referendum. Although Facebook argued that no passwords were stolen and no systems were breached, the violation of user trust and the exploitation of personal data raised serious ethical concerns about transparency and consent in data collection.

The scandal led to significant financial and reputational damage for Facebook, including a sharp decline in its stock value and fines from regulatory bodies. It also underscored the need for stronger data privacy regulations, prompting new global data protection policies such as the European Union's General Data Protection Regulation (GDPR) to prevent future misuse of personal information.

2. **Explain what the company or organization did. Did they act according to regional or national laws?**

Legal and Ethical Violations

Cambridge Analytica's actions were in violation of **Facebook's platform policies**, which prohibited developers from sharing data with third parties. Although Facebook initially allowed the quiz app to collect some data under certain terms, Cambridge Analytica **breached these terms** by transferring the data for unauthorized political use. Furthermore, Facebook itself was criticized for failing to properly monitor how third-party apps accessed and shared data.

In terms of **regional laws**:

- **In the U.S.**, there were few regulations specifically governing this type of data use at the time. However, **privacy advocates** criticized the practice for violating **users' expectations of privacy**.

- **In the U.K.**, Cambridge Analytica's operations were found to be **in breach of the Data Protection Act 1998**. The **Information Commissioner's Office (ICO)** investigated the firm and imposed fines for failing to properly handle personal data.

- The scandal prompted global regulatory responses, including the enforcement of **GDPR** in the European Union, which emphasizes the need for **explicit consent** before collecting or processing personal data.

3. **Why was the company's behavior unethical? (To answer this question, refer to this Exercise and the previous Exercise on data bias.)**

1. Lack of Informed Consent

- The data was collected through a personality quiz app under the guise of academic research. However, the true purpose—to build voter profiles for political campaigns—was not disclosed to users or their friends whose data was harvested.

- Ethical data collection requires informed consent, meaning individuals must understand what data is being collected, how it will be used, and who will have access. Cambridge Analytica failed to provide this transparency.

2. Exploitation of Data without Permission

- The company harvested data from non-users—friends of quiz participants—without their knowledge or consent. These individuals had no way to opt out or control how their personal information was used, violating principles of autonomy and privacy.

- Even though Facebook's terms prohibited such sharing, the firm proceeded with the data transfer, demonstrating a willful disregard for ethical boundaries in data usage.

3. Manipulation of Users through Targeted Bias

- The data was used to perform micro-targeting, where voters were categorized by psychological traits (e.g., neuroticism or openness). This profiling exploited users' vulnerabilities to influence political decisions through manipulative ads.

- Such profiling reflects algorithmic bias—targeted campaigns reinforced stereotypes and deepened political divisions by showing users highly curated information based on assumptions about their personality and preferences

4. Breach of Public Trust and Transparency

- Ethical organizations maintain trust with users by being transparent about data practices. Cambridge Analytica's covert use of personal information for political purposes breached this trust, damaging public confidence in technology companies like Facebook.

- Additionally, Facebook's failure to properly monitor and prevent misuse further eroded public trust and demonstrated a lack of accountability.

5. Ethical Principle of Non-Maleficence

- The principle of non-maleficence requires organizations to avoid actions that harm individuals. By using personal data without consent and manipulating users through targeted messaging, Cambridge Analytica contributed to social and political harm, including voter manipulation and the erosion of democratic processes

4. **What could the company have done to prevent this unethical behavior? Please provide some concrete suggestions.**

1. Ensure Informed Consent

- Clear and Transparent Data Collection: Cambridge Analytica should have explicitly informed users about how their data, as well as their friends' data, would be collected and used. A plain-language privacy policy and consent form would have ensured users fully understood the purpose of the data collection and its potential uses
- Granular Opt-in Options: Users should have been allowed to choose which data to share and provided with an option to prevent the collection of their friends' data.

2. Limit Data Collection and Use

- Purpose Limitation: The company should have restricted data collection to only what was necessary for legitimate research or political outreach and refrained from repurposing data without additional consent. Adhering to the principle of data minimization would have ensured ethical handling
- Separation of Political and Commercial Data: They could have created firewalls between datasets used for political campaigns and those gathered for other research purposes to prevent unethical cross-use.

3. Strengthen Data Governance and Accountability

- Internal Auditing and Compliance: Regular audits could have ensured that data-sharing practices were compliant with Facebook's platform policies and relevant privacy laws.
- Third-Party Monitoring: Employing external data auditors could have detected early misuse or policy violations, ensuring transparency throughout the data lifecycle.

4. Ethical Design of Algorithms and Data Models

- Avoid Algorithmic Bias: Cambridge Analytica should have tested its predictive models to prevent psychological manipulation and biased targeting. Incorporating ethics review boards for political data projects would have promoted fair and balanced targeting University.

- Provide Opt-out Mechanisms: Users should have had the ability to opt out of profiling and micro-targeting campaigns, safeguarding their autonomy over how data about them was used.

5. Adhere to Regulatory and Industry Standards

- Compliance with GDPR and Data Protection Laws: Even though GDPR was introduced later, Cambridge Analytica could have followed best practices for data privacy that aligned with evolving global regulations. They should have secured explicit consent for sensitive data such as political preferences
- Data Anonymization: The company could have anonymized personal data, especially for non-users, ensuring privacy even when building analytical models.

6. Build Trust through Transparency

- Public Communication and Reporting: Proactively communicating with the public about data practices and allowing users to review or delete their data would have built trust and mitigated backlash in case of a breach.
- Ethical Partnerships with Platforms: Cambridge Analytica should have maintained closer coordination with Facebook to ensure compliance with platform policies, reducing the risk of unauthorized data access

References:

“case study unethical data collection sharing company”

bing.com

Data Science Dojo — Big Data Ethics: 10 Controversial Experiments Explored

datasciencedojo.com

Dubai Lawyers — fotislaw.com

fotislaw.com

Santa Clara University — Data Collection: “Harvesting” Personalities Online - Markkula Center for Applied Ethics

scu.edu