5.3: Data Ethics: Security & Privacy

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.

- Is this a data privacy issue, data security issue, or both? Please provide a short explanation for your answer.

Answer: This situation represents both a data privacy issue and a data security issue.

Data privacy refers to the protection of individuals' personally identifiable information (PII) and ensuring that it is handled and used appropriately. In this case, the investigator taking a photo of the screen with sensitive client data is a violation of data privacy because it exposes PII to unauthorized individuals and increases the risk of potential misuse or unauthorized access to the data.

On the other hand, data security focuses on protecting data from unauthorized access, breaches, or theft. Taking a photo of the screen violates data security practices because it compromises the confidentiality and integrity of the sensitive client data. The photo could be easily shared or accessed by unauthorized individuals, potentially leading to data breaches or unauthorized use.

Therefore, this situation involves both data privacy and data security concerns as it compromises the confidentiality and privacy of sensitive client information while also potentially exposing it to unauthorized access or misuse.

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

  If the issue of investigators taking photos of sensitive client data is not addressed, there are several significant risks to Pig E. Bank and its customers:

  1. Data Privacy Breach
  2. Customer Trust
  3. Financial Loss
  5. Insider Threat
  6. Competitor Advantage

  Addressing this issue is crucial to safeguarding data privacy, maintaining customer trust, complying with regulations, and protecting the bank's reputation and financial stability.

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

  To prevent data theft, the policies around data access should be updated to prohibit any form of unauthorized data capturing or recording, including photographs or screenshots. Access privileges should be strictly controlled and limited to only those investigators who require it for their specific tasks. Implementing secure data viewing mechanisms that prevent data from being copied or saved externally would also enhance data protection. Additionally, regular training and reminders about data security protocols should be provided to all investigators to ensure they understand the importance of safeguarding sensitive client information.

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 appears to be popular with the other department

heads. Outsourcing could save the bank millions of dollars per year 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.

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

This scenario highlights a data privacy issue. Outsourcing lower-level analytical functions to a contractor in a foreign country can raise concerns about the protection and handling of sensitive customer data, such as the records of clients on active military duty and their personal identifiable information (PII). Data privacy laws vary between countries, and transferring customer data to a foreign contractor may expose the bank to compliance risks and potential violations of data privacy regulations. Ensuring that the contractor adheres to strict data privacy and security standards becomes crucial to safeguard customer information and maintain compliance with relevant laws.

- 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.

During the compliance committee meeting, I would express my concerns regarding outsourcing sensitive data to a foreign contractor. I'd emphasize that data privacy laws and regulations can vary significantly between countries, and the potential risks associated with exposing customer PII to a foreign entity must be thoroughly assessed. Specifically, I would highlight the importance of safeguarding data related to customers on active military duty, as such information could have serious implications if mishandled or accessed by unauthorized individuals. I'd recommend conducting a detailed legal and security review to ensure compliance and data protection before considering any outsourcing decision.

- 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?

To anonymize the data while enabling analysis, Pig E. Bank can apply data de-identification techniques. This involves removing or encrypting personally identifiable information (PII) such as names, addresses, and contact information. Additionally, sensitive attributes like pay grade and military status should be masked or aggregated to prevent re-identification. By transforming the data in a way that individuals cannot be directly identified, but the overall analytical value is preserved, the bank can maintain privacy compliance while allowing contractors to perform necessary analyses.

Step 3: Read the following scenario and answer the questions

Let's 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 own country where a company or organization has acted unethically in terms of collecting and sharing data. You're free to use information you find on the internet, but make sure you include the link to your resources in your document.
- Explain what the company or organization did exactly. Did they act according to regional or national laws?
- Why was the company's behavior unethical? (To answer this question, you can refer to this Exercise and the previous Exercise on data bias.)

One example of an Indian company that faced criticism for unethical data practices is the case of Aadhaar, India's biometric identification program, and its associated agency, the Unique Identification Authority of India (UIDAI).

In 2018, it was revealed that there were several instances of data breaches and mishandling of Aadhaar data. Multiple reports highlighted concerns such as unauthorized access, leakage of Aadhaar numbers, and the sale of personal information on the black market.

One notable incident involved the government-owned utility company, Bharat Sanchar Nigam Limited (BSNL). It was alleged that BSNL had allowed a private company to access and use Aadhaar data for commercial purposes without proper consent. This raised significant concerns about the misuse of sensitive personal information and violation of privacy rights.

Another controversy arose when the UIDAI filed a case against a journalist for exposing vulnerabilities in the Aadhaar system. Instead of addressing the security flaws, the authorities chose to take legal action against the whistleblower, which was widely criticized as an attempt to suppress concerns regarding the system's data protection practices.

These incidents sparked debates and led to calls for better data protection laws, stringent regulations, and increased accountability from both the government and private entities handling Aadhaar data. It highlighted the importance of ethical data collection, storage, and sharing practices to safeguard individuals' privacy and maintain public trust in such programs.

- What could you and the company have done to prevent this unethical behavior? Please provide some concrete suggestions.

To prevent unethical behavior regarding data handling, the company could have implemented the following measures:

1. Strict Data Access Controls: Limit access to sensitive data only to authorized personnel and establish a clear protocol for data access and usage.

2. Data Encryption: Utilize strong encryption techniques to protect stored data, making it difficult for unauthorized parties to access sensitive information.

3. Regular Audits: Conduct regular internal and external audits to identify potential vulnerabilities and ensure compliance with data protection regulations.

4. Employee Training: Provide comprehensive training to employees on data privacy policies, ethical practices, and the consequences of unethical behavior.

5. Independent Oversight: Have an independent body or committee to oversee data handling practices and ensure ethical compliance.

6. Consent Mechanism: Obtain explicit consent from individuals before sharing their data with third parties, ensuring transparency and accountability.

7. Strong Legal Framework: Advocate for robust data protection laws and regulations to ensure clear guidelines and penalties for non-compliance.

By implementing these measures, the company could foster a culture of ethical data handling and safeguard individuals' privacy rights.

https://www.oecd.org/gov/innovative-government/India-case-study-UAE-report-2018.pdf

https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/