Privacy & Security Academy

Title: AI Governance Workshop Case Studies

Date and Time: 23 October 2024, 9:00 AM – 12:00 ET

Presenters: Allison Levy, Taryn Crane, Karen Schuler

Group 1 Case Study: Addressing Bias in AI Tools

Background

In recent years, AI tools have become integral to various industries, from healthcare to finance. However, the deployment of these tools has raised significant concerns about bias and data leaks. This case study explores a hypothetical scenario involving an AI-driven recruitment tool used by a large multinational corporation, "TechHire Inc."

Scenario

Company: TechHire Inc.
Tool: AI-driven recruitment software
Objective: To streamline the hiring process by automatically screening resumes and ranking candidates based on their suitability for job roles.

Problem Statement

TechHire Inc. implemented an AI-driven recruitment tool to enhance efficiency and reduce human bias in the hiring process. To replicate the success of high-performing team members, they used their profiles to train the model. However, within six months of deployment, the company faced two critical issues:

1. **Bias in Candidate Selection:**
   - The AI tool consistently favored male candidates over female candidates for technical roles.
   - Candidates from certain ethnic backgrounds were underrepresented in the shortlisted pool.

Group Activity

Work with your group to:

1. Outline the steps you would take to investigate each of the critical issues.
2. Identify potential **root causes and solutions** that would improve the outcome.
3. What could be done differently in the future to avoid these issues at the start?

Group Case Study 2: Relying on AI to Produce Attorney Work Product

Background

AI has significantly transformed the legal field by streamlining the creation of attorney work products such as drafting rote documents, conducting legal research, analyzing contracts, predicting case outcomes, facilitating e-discovery and monitoring compliance. However, some tasks, even when routine, still require significant human intervention. This next case study examines the potential risks of relying too heavily on AI when producing attorney work product at the fictional medical device manufacturer known as Biotech Solutions Inc.

Scenario

BioTech Solutions is known for developing cutting-edge diagnostic equipment. The company is set to launch its latest innovation, the NeuroScan Elite, a device designed for advanced neurological diagnostics. This device has the potential to significantly enhance early detection of neurological disorders, positioning BioTech Solutions as a leader in this niche market.

As part of the launch strategy, BioTech Solutions' legal department needs to prepare a detailed legal memorandum addressing the FDA approval process and privacy compliance related to the NeuroScan Elite. Mark Davis, the in-house legal counsel, decides to leverage ChatGPT to draft the memorandum. He inputs the following prompt into the AI tool:

"Generate a comprehensive legal memorandum outlining the FDA approval process for a new medical device, including necessary steps and regulatory requirements. Additionally, address privacy compliance related to the handling of sensitive patient data collected by the device, including relevant data protection laws and best practices for securing such data."

ChatGPT then drafted a memorandum outlining the application process to obtain FDA approval for a new medical device and the privacy and security measures required under HIPPA to secure the patient data to be collected by such a device. Mark then quickly read the memorandum, and, since everything appeared to be in order, provided a copy to the General Counsel of BioTech Solutions to review with the executive team to act. As a result, Biotech Solutions filed an application with the FDA and worked to implement the privacy security measures in accordance with the memorandum.

Group Activity

Work with your group to:

1. Spot potential issues with the legal memorandum generated by ChatGPT.
2. Identify the possible consequences of following the FDA application process and implementing the privacy and security measures as outlined in memorandum.
3. Discuss ways that Chat GPT could have been used more responsibly here.

Group 3 Case Study: Addressing Security in AI Tools

Background

TechCorp, a leading technology company, integrated AI models into its customer service operations to enhance efficiency and user experience. However, the company faced significant data security challenges that exposed sensitive customer information. The system relied heavily on vast amounts of customer data to improve its accuracy and responsiveness.

Scenario

Company: TechCorp
Tool: AI-driven customer service platform
Objective: To streamline customer service by using machine learning models to analyze customer queries and provide real-time solutions.

Problem Statement

Due to time constraints, the AI model was deployed quickly without significant testing or security due diligence. In early 2023, TechCorp experienced a data breach that compromised the personal information of over 500,000 customers. The breach was traced back to vulnerabilities in the AI model's data handling processes.

Group Activity

Work with your group to:

1. Identify potential **root causes** that could have caused the issue.
2. What could be done differently in the future to avoid these issues at the start?