

Makara Ramoabi

20240045

IT Law

1. Scenario Analysis: FOI / Censorship Scenario

An FOI (Freedom of Information) scenario can be seen in a government data request system used by citizens to request public records. A user submits an online request asking for documents related to public spending on a technology project. The system logs the request and forwards it to the relevant department. Officials review the request to determine whether the information can be released or if it falls under FOI exemptions. Some sections of the documents may contain sensitive data, such as personal information or national security details, which must be redacted before release. If the request is partially or fully denied, the system provides a legal justification. This scenario shows the balance between transparency and censorship, where governments must provide access to information while protecting sensitive or restricted data.

2. Concept Research: FOI Exemptions

FOI exemptions are legal provisions that allow public authorities to withhold certain information from disclosure. These exemptions protect sensitive areas such as national security, personal privacy, law enforcement activities, and confidential commercial information. Their role is to prevent harm that could result from releasing sensitive data. Some exemptions are absolute, meaning information cannot be released, while others are qualified and require a public interest test. FOI exemptions ensure that transparency does not compromise safety, privacy, or effective government operations.

3. Tool Practice: AWS Content Moderation Reflection

AWS Content Moderation tools are designed to help organizations automatically detect and manage inappropriate or restricted content. While exploring these tools conceptually, I learned that they use machine learning to identify harmful, sensitive, or policy-violating material such as explicit images or offensive text. These tools help platforms enforce content rules consistently and at scale. The reflection highlighted how automation supports censorship and moderation efforts while reducing manual workload. AWS moderation services are useful in environments where large volumes of user-generated content must be reviewed quickly and responsibly.

4. Application Practice: Compliance Policy Explanation

A compliance policy defines how an organization handles information requests and content moderation responsibly. It outlines procedures for processing FOI requests, identifying exemptions, and applying redactions when necessary. The policy also sets standards for moderating online content in line with legal requirements and ethical guidelines. Regular audits and staff training ensure correct implementation. A strong compliance policy helps organizations balance transparency, privacy, and security while reducing legal risks. It ensures consistent decision-making and builds public trust by clearly explaining how information is managed and protected.