REVATURE

Ethics Summary

Agenda

01 Privacy

02 Security

03 Case Studies

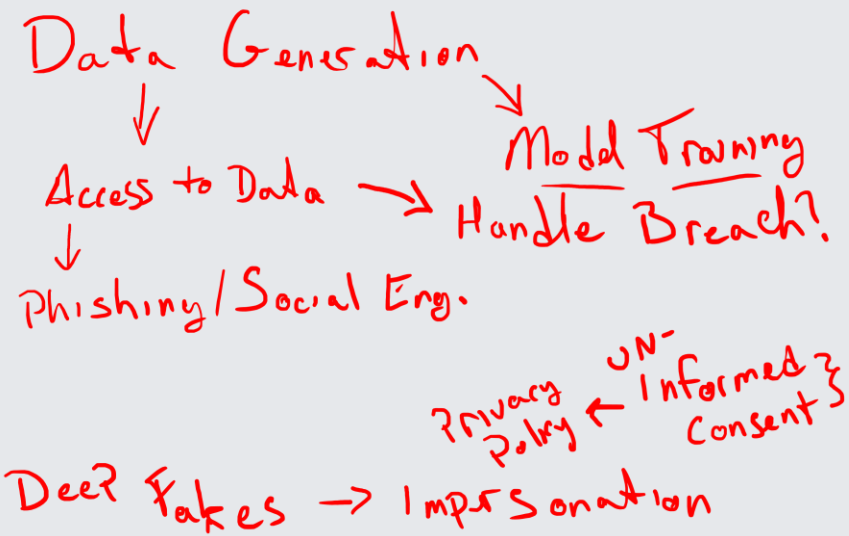
REVATURE

Privacy 

REVATURE

Privacy

What are some of the risks to privacy from AI?



How can we mitigate these risks?

- Encryption
- Informed Consent
- User Controls (opt-out)
  - Community Review
- Education / Training ← Audit/Cadence
- Data Retention ← Ethical obligation?
- Security Audits: Data Pipeline

Privacy

- Data Collection and Processing: Over collection and transparency of application.
- Anonymization: Re-Identification risk, auditing and testing.
- User Consent: Informed consent, right to erasure, opt-out.
- Usage Beyond Original Purpose: Function creep, usage transparency

Privacy by Design – Embed privacy into the design from the start and including reviews at every development stage.

Security

REVATURE

Security

- Data Storage: Access controls, encryption, breach reporting
- Third-Party Dependency: Vendor compliance, vendor systems, transfers
- Continuous Monitoring: Regular updates, periodic audits
- Incident Response: Detect, notify, investigate, implement
- Staff Training: Threat detection and security best practices

Case Studies

REVATURE

Case Studies

https://www.enzuzo.com/blog/ai-privacy-violations

https://www.ibm.com/think/insights/ai-privacy

Overview

- Was data collected or handled in a way that violated the law or best practices?
- Was there malicious intent in how data was handled?
- What were the results of this event?
- What could have been done to avoid or mitigate this event?

Thank You!

REVATURE