Mark Meyer

Assistant State Privacy Officer

This is for educational purposes only

Office of the

State Auditor

Privacy Academy

- 60+ participants over the 7-week course.
  - 48 participants took and passed the final exam.

- Planning a Spring 2025 Session.
  - Based on survey results:
    - Course length will expand to 10-weeks.
    - Each module will expand to 90 minutes (from 60 minutes).

Mobile Apps Privacy Assessment

SCOPE:

- Mobile apps developed and / or published by governmental entities.
- Over 700 apps identified

HOW:

- Determined by the governmental entity URL linked in the app store.

WHAT:

- Targeted review of privacy policy statements and “privacy labels” of apps collecting sensitive data.
- Review of “data linked to you” “data used to track you” and “data not linked to you” transparency and internal logic.

Red Flags Observed

- Missing or misleading privacy policies.
  - "Privacy policy" link leads to the entity's copyright page
  .
- Non-specific data points.
  - E.g., "Identifiers", "Other Data", "Files".

- Lack of transparency in data sharing practices.
  - Not stating whether data is shared
  - Stating data is shared, but not what data.

- Suspected Overcollection of personal data
  - App collects data elements that are not obviously needed for the core function of the app to work.

Inherent Risk Focus

Apps that inherently process high-risk (sensitive) data by the nature of the app. Typically found in:

- Healthcare
- Education
- Law Enforcement

Examples of apps reviewed:

(Canvas, SafeUT, Care@Work, Layton City, Salt Lake City School District)

Next Steps

- Approach developers / publishers of Apps classified as inherently sensitive and presenting more than 1 red flag first.

- Conduct a deep-dive review of how the privacy statement and privacy labels correspond with actual data collection and use.

- Focus on over-collection, over-retention and over-sharing as well as data aggregation/ anonymization standards used.

Recommendations for Entities

- Build with “privacy by design and default” mindset.
- Conduct privacy impact assessments.
  - Review ethical use of data, transparency, identify gaps in privacy policies, data collection practices, and regulatory compliance before the app is published.
- Develop clear and specific data privacy policies/statements
  - Apps should identify exact data points collected.
- Implement detailed data sharing disclosures.
  - Apps should identify with whom the data is shared and the purpose of sharing and offer **opt-in** as opposed to opt out.

Goals Moving Forward

- Focus on reviews and audits
  - Primary Focus:
    - Law Enforcement Data
    - Healthcare Data
    - Use of AI

- Auditing against GDPA for the existence of Privacy Programs as of May 2025