Privacy for Airport Law Enforcement

Nora Kurzova
Asst. State Privacy Officer,
State of Utah

Office of the
State Auditor

Privacy as a Concept

- What is “Personal data”?

  “Any information that can be used, directly or indirectly, to identify a living individual”

- Lets see how easy it is to identify an individual based on generic data…

Identification Game

WOMAN

CZECH NATIONAL

PRIVACY LAWYER

Lets Talk About AI

- What AI are we talking about?

  “Narrow / Weak AI” (including generative AI), AI that is not “general”, not self-aware, not surpassing the capability of a human mind.

- Why do we care?

  If used incorrectly, it can present variety of bias, lead to skewed results, become intrusive or manipulative, or aid criminals.

Airport security potential application of AI and new technologies

- Passenger identification via biometrics
- Passenger flow management
- Less intrusive Passenger body scanning
- More precise luggage scanning
- Predicting breaches of security
- Predicting maintainance needs
- Predicting passenger density
- More accurate calculation of flight delays

Common privacy concerns people raise against AI

- I find it intrusive
- I find it unexpected
- I find it non transparent
- I think it manipulates me
- I cannot control its settings
- I think it discriminates against me
- The data can leak/be stolen and abused
- It harvests my data and sells it onward

What can you do to aleviate these concerns?

- I find it intrusive – Privacy Impact Assessment
- I find it unexpected – Privacy notice
- I find it non transparent – Privacy Policy
- It manipulates me – Ethical use of data policy
- I cannot control its settings – Privacy by D&D
- It discriminates – PIA with extra Bias check
- It harvests my data and sells it onward – ban on monetization (or exchange) of the data.
- The data can leak/be stolen and abused – PIA, and a retention policy with enforced deletion.

Airline Data Leak 2023

- In 2023, the TSA investigated a “potential cybersecurity incident” after someone claimed to have discovered an airline “no-fly” list on an unsecure server.
- The person who discovered the server described herself as a cybersecurity researcher” and notified the airline.
- The airline confirmed it was true and the unsecure server included an older version of the list with names and birthdates.

Use of Facial Recognition

- Growing number of airports use opt-in facial recognition to identify a passenger. Current claim is 99% accuracy across all demographic groups per TSA.
- Cases of false results (not at airports) resulted in arrests and other erroneous conduct by Law Enforcement, especially toward people of color. Trust was harmed.
- How can we improve the situation? Rebuild trust via enhanced transparency.

What is a Privacy Impact Assessment (PIA) and when do you do it?

It's a process that evaluates potential adverse impact on personal privacy and analyzes if risk is adequately mitigated

You conduct a PIA when your entity plans a new project or process which includes:

A) Large amount of personal data

B) Sensitive personal data

C) Novel technologies, such as AI

Any other time you want, or the law says so.

Basic questions for a PIA

- What do you use the data for? (limit)
- Who can legitimately access it?
- How do you protect it from abuse? (guard)
- Whats the worst that can happen?
- How do you prevent it?
- Do you have all documents in place?
- Do you follow Privacy by DnD?
- When do you delete the data? (delete)
- How do you monitor compliance?

Deeper Look at real PIAs:

From the Dept. of Homeland Security PIAs on use of Facial Recognition:

"Passengers must take multiple steps to opt-in, including affirmative steps during their check-in process before and during photograph capture."

"During the check-in process, passengers will opt-in and consent to providing PII prior to the pre-stage of their photograph and confirm that they have read a Privacy Notice."

Deeper Look at real PIAs:

Privacy Risk:

There is a risk that passengers will not know that TSA is taking their photographs for identity verification.

Mitigation claim: This risk is mitigated.

In order to be eligible for this process, the passenger must take several steps, and pose for the live photo in front of the camera. TSA provides signage…

Transparency of Notice and Validity of Consent:

TSA: ”camera only turns on when a person puts in their ID card — so it’s not randomly gathering images of people at the airport.”

Q: How do those that have not read the article or studied the notice and policy know that??.

Additional Passenger concerns:

- Will me saying “No” cause trouble for me?
- What have I just consented to? (how easy was it to understand?)

More resources to ensure Privacy Risk is adequately mitigated

- NIST framework

  https://www.nist.gov/cyberframework

- DOJ PIAS

  https://www.justice.gov/opcl/doj-privacy-impact-assessments

- Utah State Privacy Office

  https://auditor.utah.gov/privacy/

- IAPP resouces

  https://iapp.org/resources/

Takeaways and questions

- Evaluate Need vs. Impact
- Honor Transparency and Simplicity,
- Employ the “Grandmother test”
- Conduct Privacy Impact Assessments
- Focus on enhanced communication
- Follow the “Limit, Guard, Delete” rule
- Train people and Monitor processes.

Thank you.

Nora Kurzova nkurzova@utah.gov