Lightweight Purpose Justification Service for Embedded Accountability

PEPR 2021

Arnav Jagasia + Yeong Wei Wee
Privacy and Civil Liberties, Palantir Technologies
Lightweight Purpose Justification Service for Embedded Accountability

PEPR 2021

Arnav Jagasia + Yeong Wei Wee
Privacy and Civil Liberties, Palantir Technologies
What we do

The goal of the Privacy and Civil Liberties (PCL) team is to design, build, and deploy privacy-protective technologies, and to foster a culture of responsibility around their development and use.
Purpose Limitation in Practice - Lightweight Purpose Justification
Service for Embedded Accountability
Purpose Limitation

- Data must be collected for specified, explicit and legitimate purposes only
Purpose Limitation

→ Data must be collected for specified, explicit and legitimate purposes only

→ Data must not be further processed in a way that is incompatible with those purposes
Challenges for Governance

→ Legal Reviews
→ Privacy Impact Assessments
→ Access Controls
→ Audit Log Analysis

Data platform

Governance
Challenges for Users

→ Legal Reviews
→ Privacy Impact Assessments
→ Access Controls
→ Audit Log Analysis

→ Tooling for purpose limitation in daily routine
→ Interfaces that “bake in” organizational policy
→ Active reminders and nudges
Gap in practice

→ Legal Reviews
→ Privacy Impact Assessments
→ Access Controls
→ Audit Log Analysis

Data platform

→ Tooling for purpose limitation in daily routine
→ Interfaces that “bake in” organizational policy
→ Active reminders and nudges
Embedding Accountability
Governance configuration

- Select the platform actions to checkpoint
- Configure language and justification requirements for the actions
→ When performing sensitive action, served with checkpoint
→ Requires acknowledgement and justification
→ Reminder of policy and purposes
→ Reminder that justifications and actions are auditable
Governance review

→ Real-time review of history of user actions and corresponding context

→ Determine from justifications and metadata whether purposes appropriate

You are viewing the first 15 checkpoints that match this search. Click here to load more.

Data is notional
Embedded accountability

mutually reinforcing

Governance

Platform User

Data platform
Embedded accountability

mutually reinforcing

Governance

Platform User

Data platform

Developer
Technical Facets of the Purpose Justification Framework
Enforcing purpose limitation in a platform backed by microservices can be quite challenging.
The purpose justification framework has a few key goals:

1. **Governance users** can configure justification checkpoints for actions they deem sensitive.
2. When a **platform user** performs a sensitive action, the user sees the configured checkpoint and submits a user justification.
3. **Governance users** can review the sensitive actions users have taken along with the justification and the context for the sensitive action.
Purpose Justification Framework Overview

→ We designed a lightweight purpose justification service with a few simple API endpoints to meet these goals.

1. **Governance users** can configure justification checkpoints for actions they deem sensitive.

2. When a **platform user** performs a sensitive action, the user sees the configured checkpoint and submits a user justification.

3. **Governance users** can review the sensitive actions users have taken along with the justification and the context for the sensitive action.

createConfiguration
getConfiguration
putJustification
getJustifications
Frontend Governance Workflows

PEPR 21 – Lightweight Purpose Justification Service for Embedded Accountability

June 2021
Frontend Governance Workflows: Configuration
Frontend Governance Workflows: Review

PEPR 21 – Lightweight Purpose Justification Service for Embedded Accountability

June 2021
We propose an object model for such a “sensitive action” that as a few key parts:

- **Action Type** - an intuitive name for the action that was performed (“File Import”, “Dataset Export”, “De-obfuscate”, etc.)
- **Acting User** - the user who performed the action
- **Related Items** - data that is associated with the sensitive action (ex: the dataset that was exported, the files a user uploaded, etc.)
- **Prompt** - the prompt the user was presented with when the user was asked for a justification
- **User Justification** - the justification that the user provided
Access controls can help solve some of these security challenges:

- Access to User Interface for Viewing Justifications
- All-Encompassing Access in the Platform
- Balancing New Risks to Employee Privacy
Technical Takeaways

- **Simple APIs** for configuring, displaying, and reviewing justification prompts and user-submitted justifications

- Purpose Justification **Object Model**

- **Generalized Architecture** for Purpose Justification Framework

**Purpose Justification Framework Starter Kit**

- APIs
- Object Model
- Architecture
Outcomes and feedback

→ Greater awareness and context of user activity
→ Flag gaps in existing accountability procedures
→ Improve processes and training over time
Outcomes and feedback

- Greater awareness and context of sensitive user activity
- Flag gaps in existing accountability procedures
- Improve processes and training over time

→ Reminder and nudge of sensitive action
→ Organizational policy at fingertips at action-time
→ When unsure, have an escalation path to check
### Outcomes and feedback

- Greater awareness and context of sensitive user activity
- Flag gaps in existing accountability procedures
- Improve processes and training over time
- Reminder and nudge of sensitive action
- Organizational policy at fingertips at action-time
- When unsure, have an escalation path to check

#### Governance

- Medicine

#### Platform

- Organizational policy

#### Data platform

- Low code complexity doesn’t slow product velocity
- Low maintenance burden

- Ease of integration

- Mutual reinforcing
Outcomes and feedback

→ Greater awareness and context of sensitive user activity
→ Flag gaps in existing accountability procedures
→ Improve processes and training over time

→ Reminder and nudge of sensitive action
→ Organizational policy at fingertips at action-time
→ When unsure, have an escalation path to check

→ Ease of integration
→ Low code complexity doesn’t slow product velocity
→ Low maintenance burden

PEPR 21 – Lightweight Purpose Justification Service for Embedded Accountability
June 2021
Lightweight Purpose Justification Service for Embedded Accountability

PEPR 2021

Arnav Jagasia + Yeong Wei Wee
Privacy and Civil Liberties, Palantir Technologies