

# 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

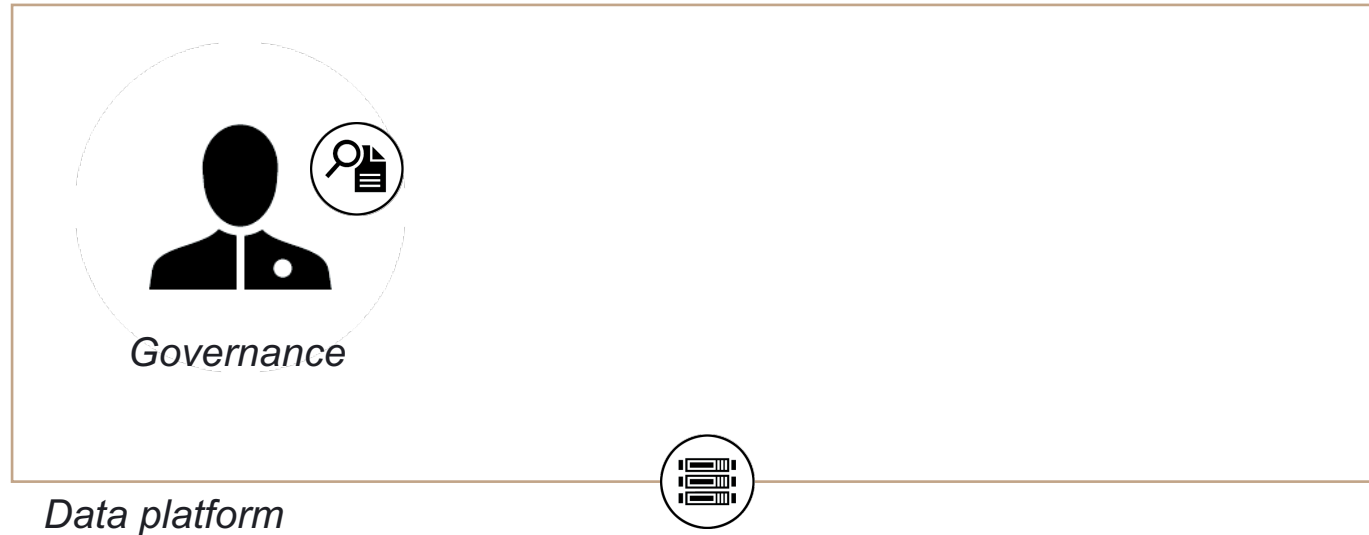
- Data must be collected for specified, explicit and legitimate purposes only

# 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

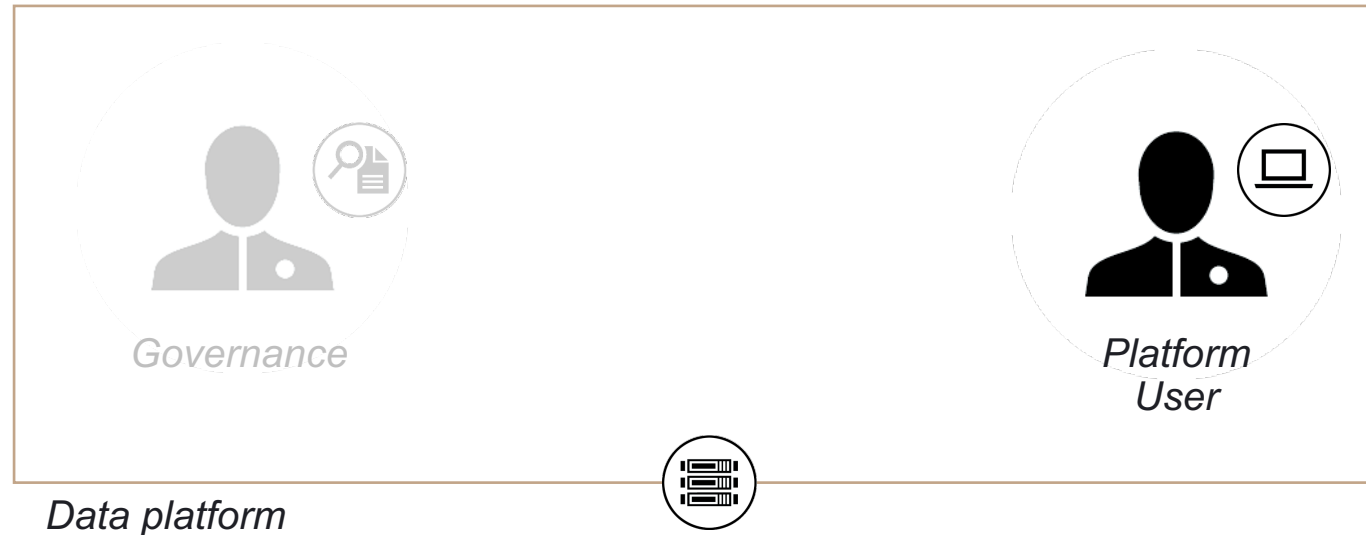
- Legal Reviews
- Privacy Impact Assessments
- Access Controls
- Audit Log Analysis





# Challenges for Users

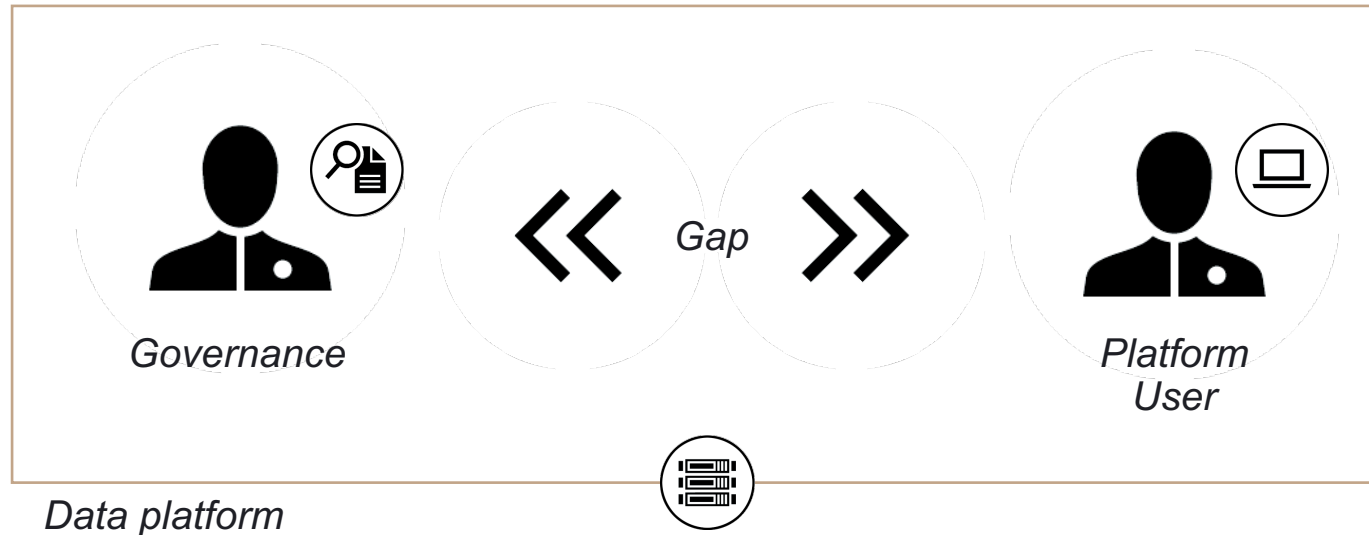
- Legal Reviews
- Privacy Impact Assessments
- Access Controls
- Audit Log Analysis



- 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

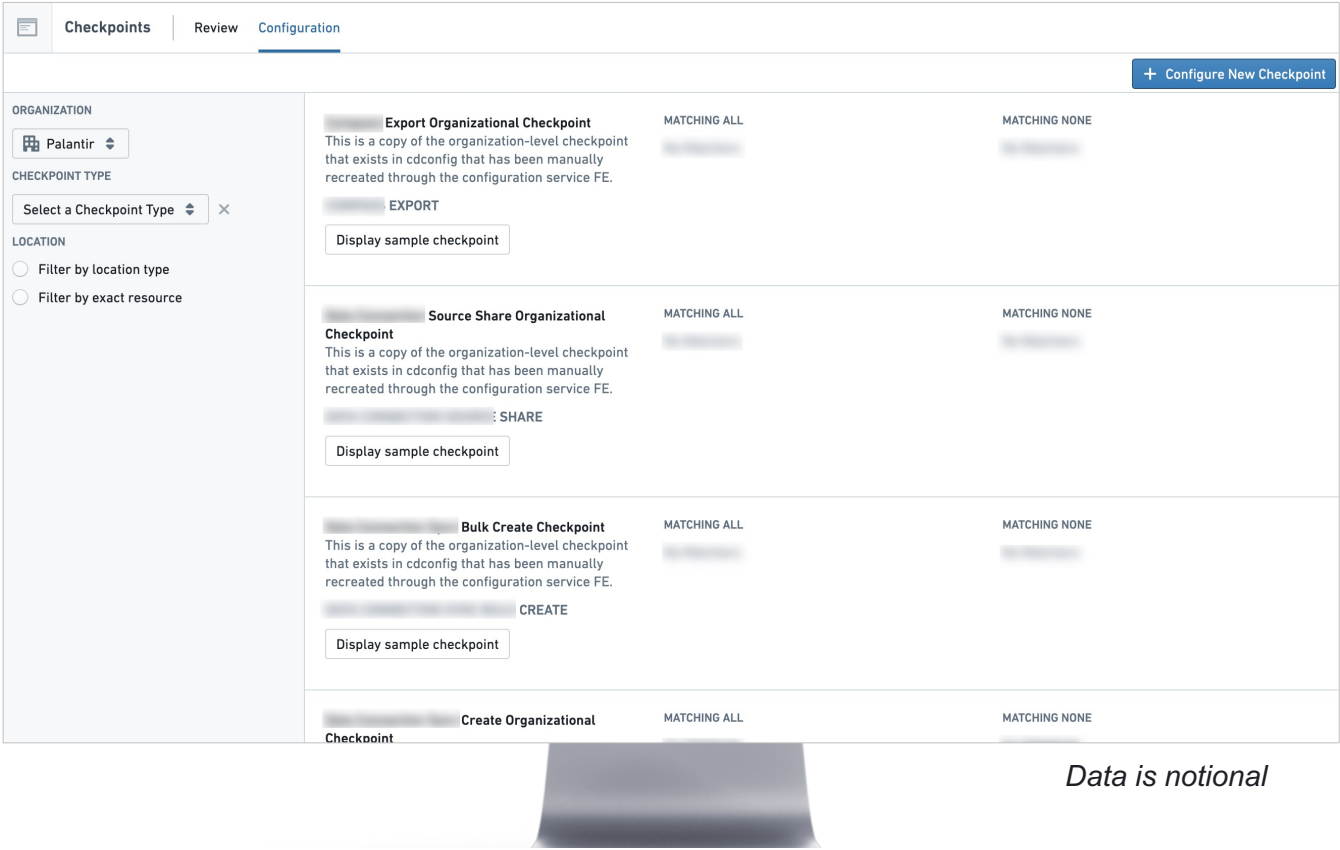


- Tooling for purpose limitation in daily routine
- Interfaces that “bake in” organizational policy
- Active reminders and nudges

# Embedding Accountability

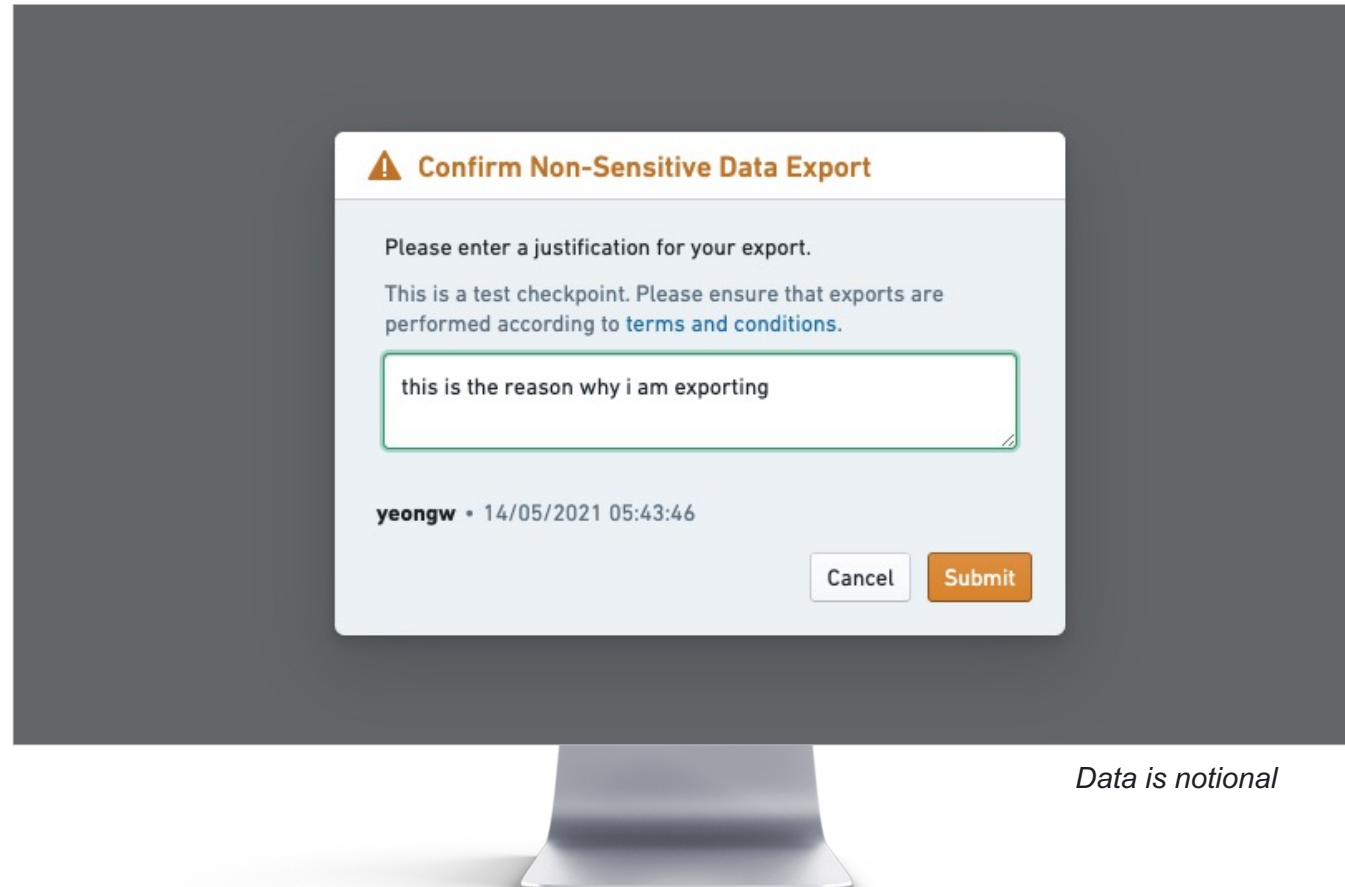
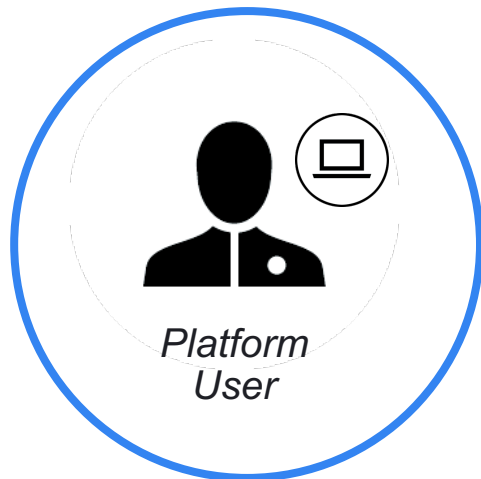
# Governance configuration

- Select the platform actions to checkpoint
- Configure language and justification requirements for the actions



# User checkpointing

- When performing sensitive action, served with checkpoint
- Requires acknowledgement and justification
- Reminder of policy and purposes
- Reminder that justifications and actions are auditable



*Data is notional*



# Governance review

- Real-time review of history of user actions and corresponding context
- Determine from justifications and metadata whether purposes appropriate



Checkpoints

ORGANIZATION

Governance

SEARCH FILTER

Select a Filter

TIME INTERVAL

Tue Mar 09 2021

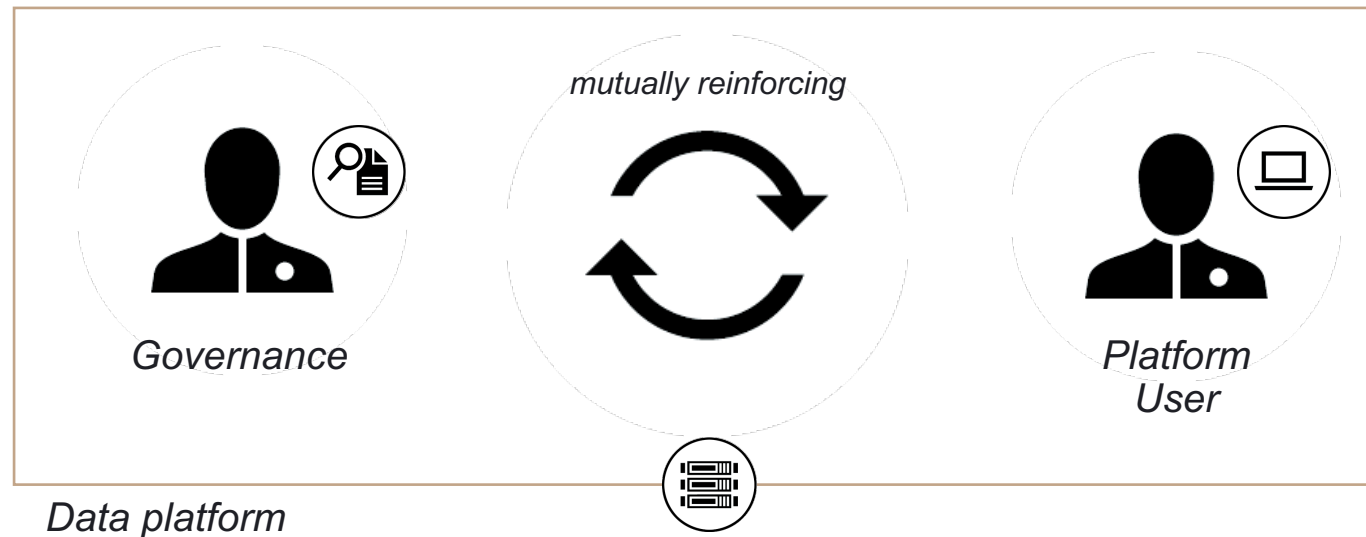
Fri Mar 12 2021

Time	Type	User	Justification	Checkpointed Items	Project	Selected Checkpoint Details
Mar 11, 2021, 2:21 PM	Export	Governance Admin	I agree download png	Screen Shot 2021-03... /Users/governance_admin	governance_admin /Users	<div>User Justification I agree I'm not ingesting PII</div> <div>Checkpoint Prompt Unknown Prompt</div> <div>Creation Time Mar 10, 2021, 5:09 PM</div> <div>Checkpoint Type Data Connection Sync Create</div> <div>Acting User brian_gov</div> <div>Username</div> <div><div>CHECKPOINTED ITEM</div><div>Checkpoints Demo Source /demo/Privacy &amp; Governance/Checkpoints Demo</div><div>Resource Type Source</div><div>Name Checkpoints Demo Source</div><div>Path /demo/Privacy &amp; Governance/Checkpoints De...</div><div>Project Privacy &amp; Governance</div></div> <div><div>CHECKPOINTED ITEM</div><div>Redacted Resource</div><div>Resource Type Sync</div><div>Name Redacted Name</div><div>Path Redacted Path</div></div> <div>Checkpoint Version 1</div>
Mar 11, 2021, 2:21 PM	Import	Governance Admin	Checkbox Ticked	Screen Shot 2021-03... /Users/governance_admin	governance_admin /Users	
Mar 11, 2021, 2:20 PM	Export	Governance Admin	test I agree	employee_registry /Users/governance_admin	governance_admin /Users	
Mar 11, 2021, 12:59 PM	Export	Jane Taylor	I agree to the rules	monthly_account_acti... /demo/Privacy & Govern...	Privacy & Governance /demo	
Mar 11, 2021, 12:38 PM	Import	Jane Taylor	Checkbox Ticked	all_accounts (5) /demo/Privacy & Govern...	Privacy & Governance /demo	
Mar 11, 2021, 12:06 PM	Import	Jane Taylor	Checkbox Ticked	all_accounts (4) /demo/Privacy & Govern...	Privacy & Governance /demo	
Mar 11, 2021, 10:45 AM	Export	Jane Taylor	I agree	monthly_account_acti... /demo/Privacy & Govern...	Privacy & Governance /demo	
Mar 11, 2021, 10:05 AM	Import	Jane Taylor	Checkbox Ticked	all_accounts (3) /demo/Privacy & Govern...	Privacy & Governance /demo	
Mar 11, 2021, 9:42 AM	Export	Jane Taylor	I agree	monthly_account_acti... /demo/Privacy & Govern...	Privacy & Governance /demo	
Mar 11, 2021, 9:14 AM	Import	Jane Taylor	Checkbox Ticked	all_accounts (2) /demo/Privacy & Govern...	Privacy & Governance /demo	
Mar 10, 2021, 5:14 PM	Import	Brian Jordan	Checkbox Ticked	Redacted Resource	Redacted Resource	
Mar 10, 2021, 5:12 PM	Import	Governance Admin	Checkbox Ticked	employee_registry /Users/governance_admin	governance_admin /Users	
Mar 10, 2021, 5:09 PM	Create	Brian Jordan	I agree I'm not ingesting PII	Checkpoints Demo So... /demo/Privacy & Govern...	Privacy & Governance /demo	
Mar 10, 2021, 5:08 PM	Create	Brian Jordan	Saving my personal sync. I ...	Checkpoints Demo So... /demo/Privacy & Govern...	Privacy & Governance /demo	
Mar 10, 2021, 5:07 PM	Export	Jane Taylor	Downloading obfuscated e...	all_accounts_protected /demo/Privacy & Govern...	Privacy & Governance /demo	

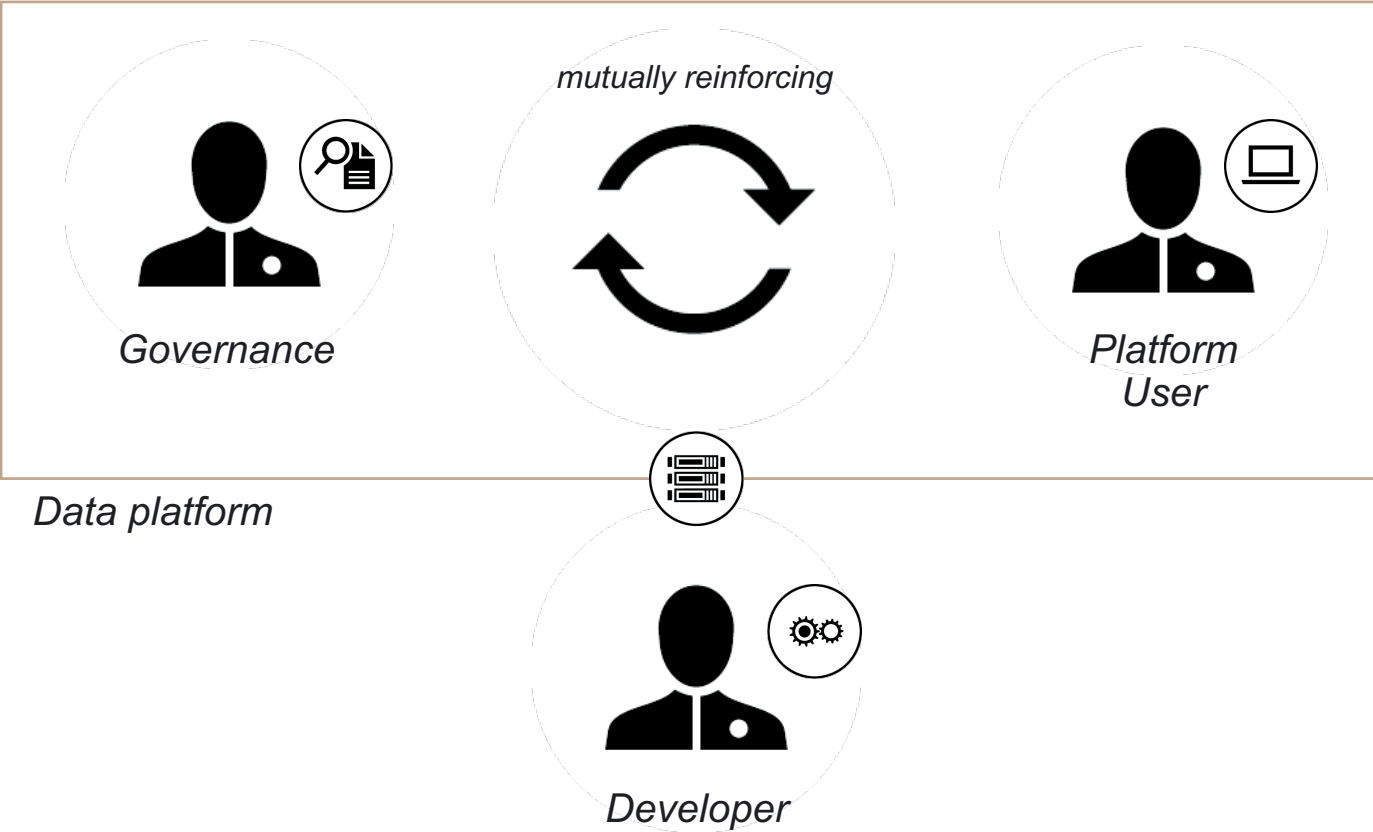
You are viewing the first 20 checkpoints that match this search. Click here to load more.

Data is notional

# *Embedded accountability*



# Embedded accountability

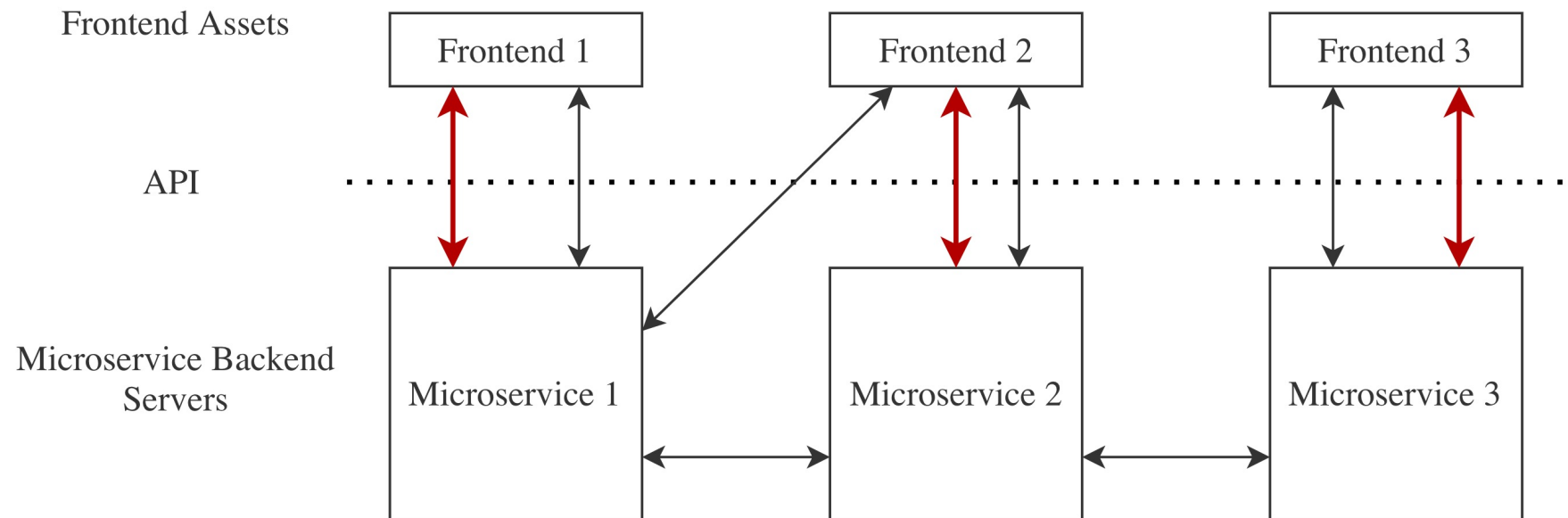


# Technical Facets of the Purpose Justification Framework

# Background: Microservice Environment

- Enforcing purpose limitation in a platform backed by microservices can be quite challenging.

## Microservice Architecture Design

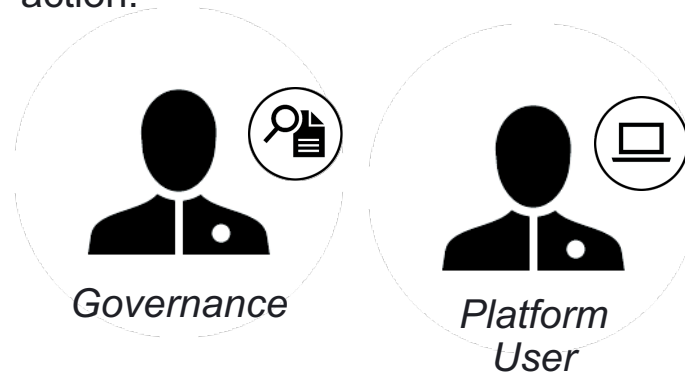




# Purpose Justification Framework Overview

→ 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.

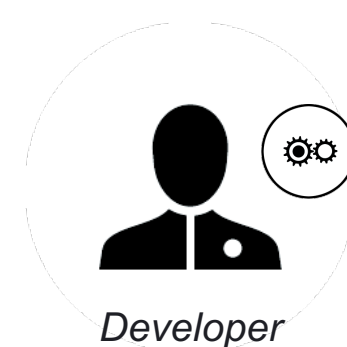
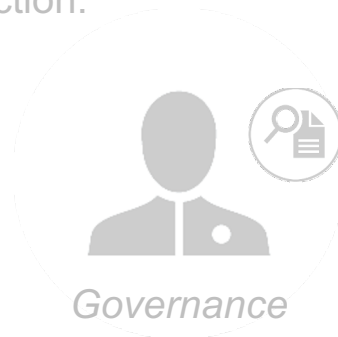
1. **Governance users** can configure justification checkpoints for actions they deem sensitive.
2. When a **platform user** performs a sensitive action, the user sees the configured checkpoint and submits a user justification.
3. **Governance users** can review the sensitive actions users have taken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

`createConfiguration`

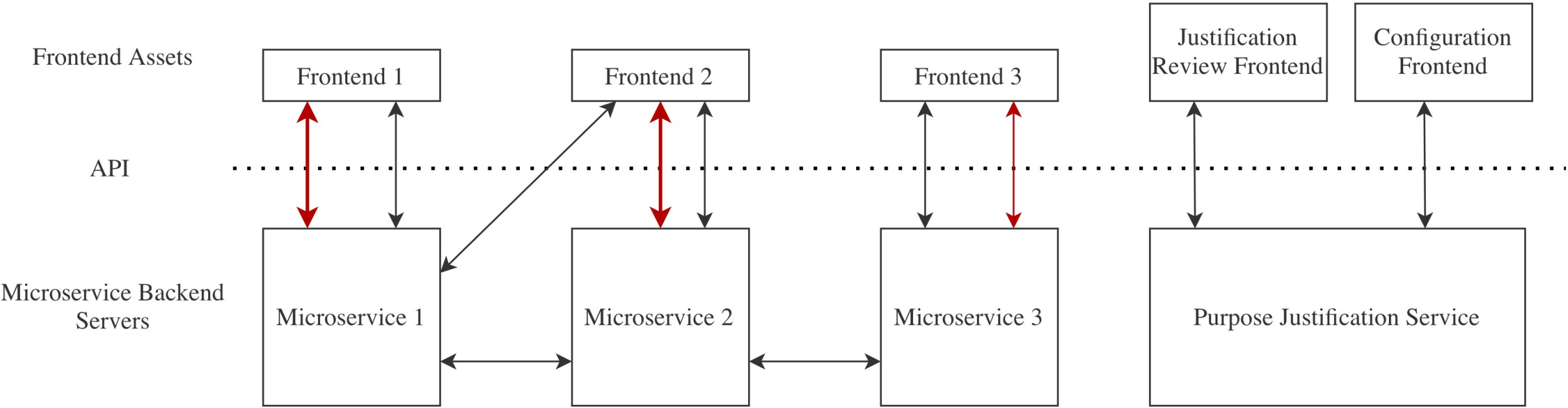
`getConfiguration`

`putJustification`

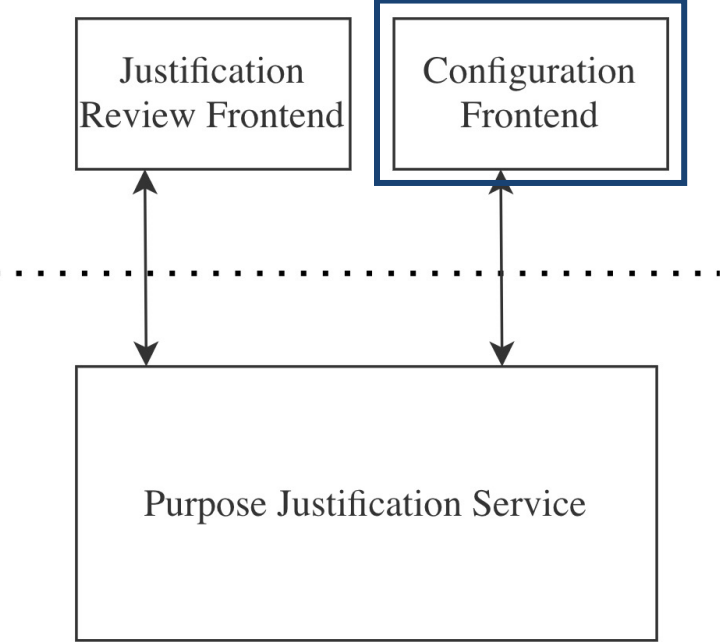
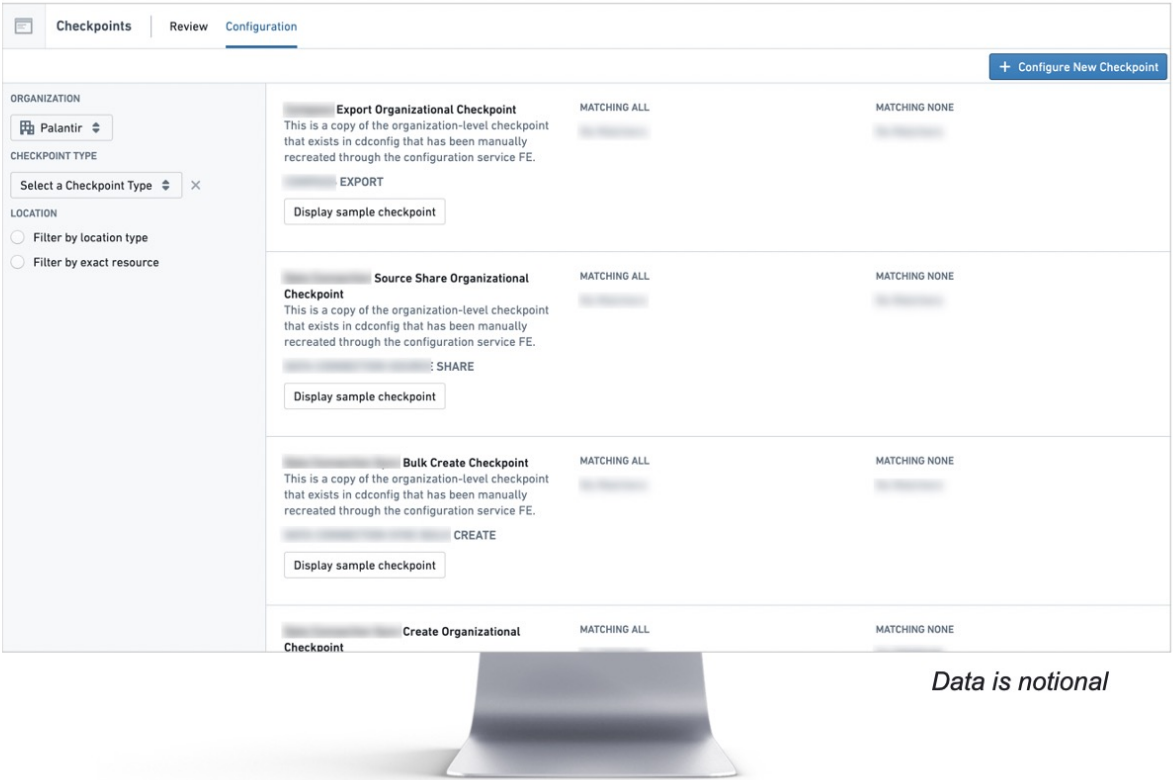
`getJustifications`



# Frontend Governance Workflows



# Frontend Governance Workflows: Configuration



# Frontend Governance Workflows: Review

Checkpoints

ORGANIZATION Governance

SEARCH FILTER

Select a Filter

TIME INTERVAL Tue Mar 09 2021 Fri Mar 12 2021

Time	Type	User	Justification	Checkpointed Items	Project
Mar 11, 2021, 2:21 PM	Export	Governance Admin	I agree download png	Screen Shot 2021-03-11 2:21 PM /Users/governance_admin /Users	governance_admin /Users
Mar 11, 2021, 2:21 PM	Import	Governance Admin	Checkbox Ticked	Screen Shot 2021-03-11 2:21 PM /Users/governance_admin /Users	governance_admin /Users
Mar 11, 2021, 2:20 PM	Export	Governance Admin	test I agree	employee_registry /Users/governance_admin /Users	governance_admin /Users
Mar 11, 2021, 12:59 PM	Export	Jane Taylor	I agree to the rules	monthly_account_acti... /demo/Privacy & Govern... /demo	Privacy & Governance /demo
Mar 11, 2021, 12:38 PM	Import	Jane Taylor	Checkbox Ticked	all_accounts (5) /demo/Privacy & Govern... /demo	Privacy & Governance /demo
Mar 11, 2021, 12:06 PM	Import	Jane Taylor	Checkbox Ticked	all_accounts (4) /demo/Privacy & Govern... /demo	Privacy & Governance /demo
Mar 11, 2021, 10:45 AM	Export	Jane Taylor	I agree	monthly_account_acti... /demo/Privacy & Govern... /demo	Privacy & Governance /demo
Mar 11, 2021, 10:05 AM	Import	Jane Taylor	Checkbox Ticked	all_accounts (3) /demo/Privacy & Govern... /demo	Privacy & Governance /demo
Mar 11, 2021, 9:42 AM	Export	Jane Taylor	I agree	monthly_account_acti... /demo/Privacy & Govern... /demo	Privacy & Governance /demo
Mar 11, 2021, 9:14 AM	Import	Jane Taylor	Checkbox Ticked	all_accounts (2) /demo/Privacy & Govern... /demo	Privacy & Governance /demo
Mar 10, 2021, 5:14 PM	Import	Brian Jordan	Checkbox Ticked	Redacted Resource	Redacted Resource
Mar 10, 2021, 5:12 PM	Import	Governance Admin	Checkbox Ticked	employee_registry /Users/governance_admin /Users	governance_admin /Users
Mar 10, 2021, 5:09 PM	Create	Brian Jordan	I agree I'm not ingesting PII	Checkpoints Demo So... /demo/Privacy & Govern... /demo	Privacy & Governance /demo
Mar 10, 2021, 5:08 PM	Create	Brian Jordan	Saving my personal sync. I ...	Checkpoints Demo So... /demo/Privacy & Govern... /demo	Privacy & Governance /demo
Mar 10, 2021, 5:07 PM	Export	Jane Taylor	Downloading obfuscated e...	all_accounts_protected /demo/Privacy & Govern... /demo	Privacy & Governance /demo

You are viewing the first 20 checkpoints that match this search. Click here to load more.

Selected Checkpoint Details

User Justification I agree I'm not ingesting PII

Checkpoint Prompt Unknown Prompt

Creation Time Mar 10, 2021, 5:09 PM

Checkpoint Type Data Connection Sync Create

Acting User Username brian\_gov

CHECKPOINTED ITEM Checkpoints Demo Source /demo/Privacy & Governance/Checkpoints Demo

Resource Type Source

Name Checkpoints Demo Source

Path /demo/Privacy & Governance/Checkpoints De...

Project Privacy & Governance

CHECKPOINTED ITEM Redacted Resource

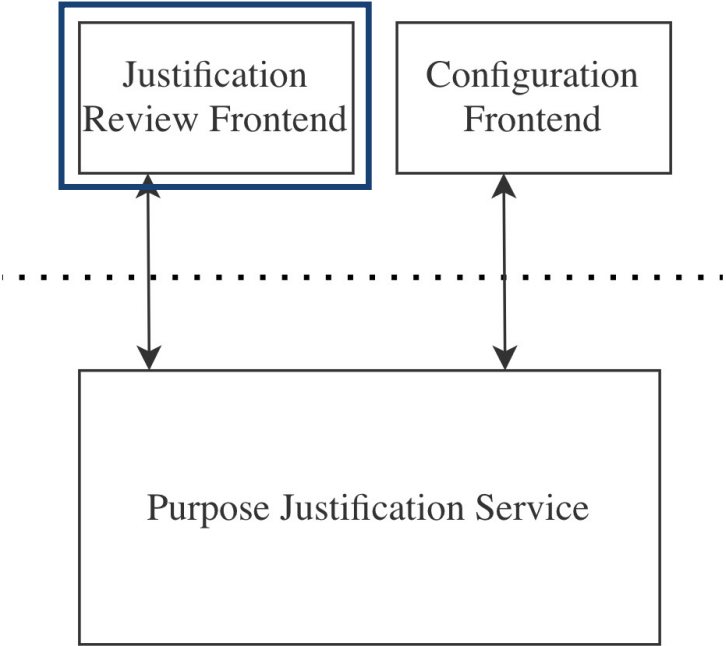
Resource Type Sync

Name Redacted Name

Path Redacted Path

Checkpoint Version 1

Data is notional

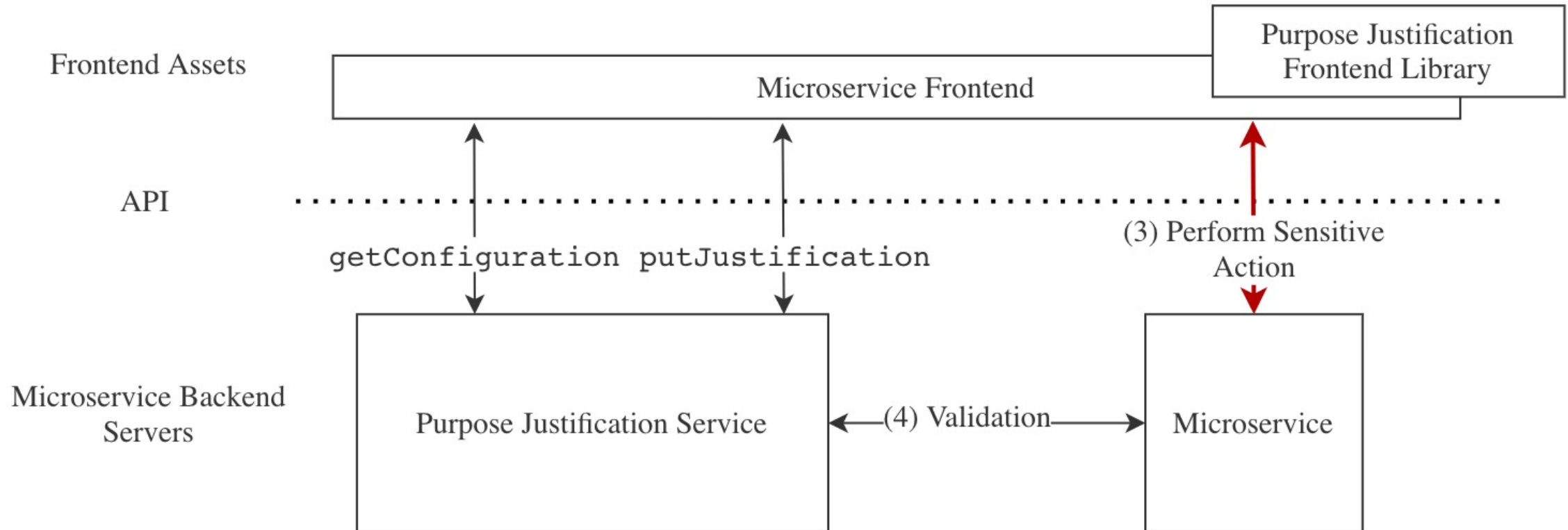




# Modeling Purpose Justifications

- 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

# Generalized Architecture



# Challenges in Security and Access Control

Checkpoints						
ORGANIZATION		SEARCH FILTER	Select a Filter	TIME INTERVAL		
Governance				Tue Mar 09 2021 Fri Mar 12 2021		
Time	Type	User	Justification	Checkpointed Items	Project	Selected Checkpoint Details
Mar 11, 2021, 2:21 PM	Export	Governance Admin	I agree download png	Screen Shot 2021-03-11 2:21 PM /Users/governance_admin	governance_admin /Users	User Justification I agree I'm not ingesting PII
Mar 11, 2021, 2:21 PM	Import	Governance Admin	Checkbox Ticked	Screen Shot 2021-03-11 2:21 PM /Users/governance_admin	governance_admin /Users	Checkpoint Prompt Unknown Prompt
Mar 11, 2021, 2:20 PM	Export	Governance Admin	test I agree	employee_registry /Users/governance_admin	governance_admin /Users	Creation Time Mar 10, 2021, 5:09 PM
Mar 11, 2021, 12:59 PM	Export	Jane Taylor	I agree to the rules	monthly_account_acti... /demo/Privacy & Govern...	Privacy & Governance /demo	Checkpoint Type Data Connection Sync Create
Mar 11, 2021, 12:38 PM	Import	Jane Taylor	Checkbox Ticked	all_accounts (5) /demo/Privacy & Govern...	Privacy & Governance /demo	Acting User brian_gov
Mar 11, 2021, 12:06 PM	Import	Jane Taylor	Checkbox Ticked	all_accounts (4) /demo/Privacy & Govern...	Privacy & Governance /demo	Username
Mar 11, 2021, 10:45 AM	Export	Jane Taylor	I agree	monthly_account_acti... /demo/Privacy & Govern...	Privacy & Governance /demo	CHECKPOINTED ITEM
Mar 11, 2021, 10:05 AM	Import	Jane Taylor	Checkbox Ticked	all_accounts (3) /demo/Privacy & Govern...	Privacy & Governance /demo	Checkpoints Demo Source /demo/Privacy & Governance/Checkpoints Demo
Mar 11, 2021, 9:42 AM	Export	Jane Taylor	I agree	monthly_account_acti... /demo/Privacy & Govern...	Privacy & Governance /demo	Resource Type Source
Mar 11, 2021, 9:14 AM	Import	Jane Taylor	Checkbox Ticked	all_accounts (2) /demo/Privacy & Govern...	Privacy & Governance /demo	Name Checkpoints Demo Source
Mar 10, 2021, 5:14 PM	Import	Brian Jordan	Checkbox Ticked	Redacted Resource	Redacted Resource	Path /demo/Privacy & Governance/Checkpoints De...
Mar 10, 2021, 5:12 PM	Import	Governance Admin	Checkbox Ticked	employee_registry /Users/governance_admin	governance_admin /Users	Project Privacy & Governance
Mar 10, 2021, 5:09 PM	Create	Brian Jordan	I agree I'm not ingesting PII	Checkpoints Demo So... /demo/Privacy & Govern...	Privacy & Governance /demo	CHECKPOINTED ITEM
Mar 10, 2021, 5:08 PM	Create	Brian Jordan	Saving my personal sync. I...	Checkpoints Demo So... /demo/Privacy & Govern...	Privacy & Governance /demo	Redacted Resource
Mar 10, 2021, 5:07 PM	Export	Jane Taylor	Downloading obfuscated e...	all_accounts_protected /demo/Privacy & Govern...	Privacy & Governance /demo	Resource Type Sync
You are viewing the first 20 checkpoints that match this search. Click here to load more.						
Checkpoint Version 1						



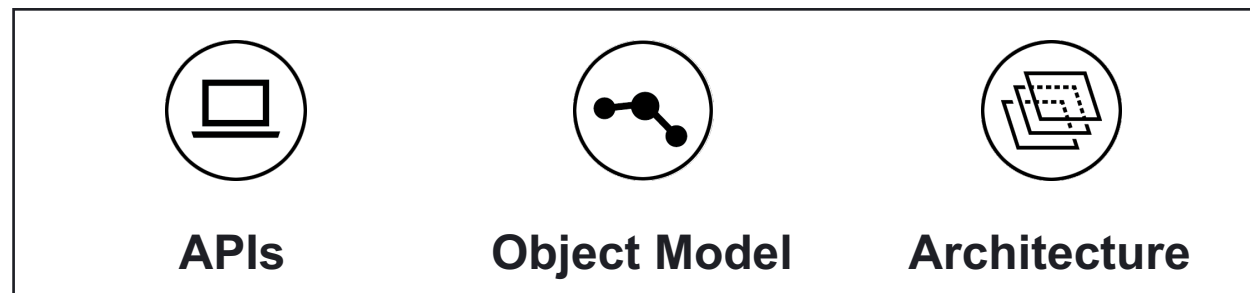
Data is notional

- 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

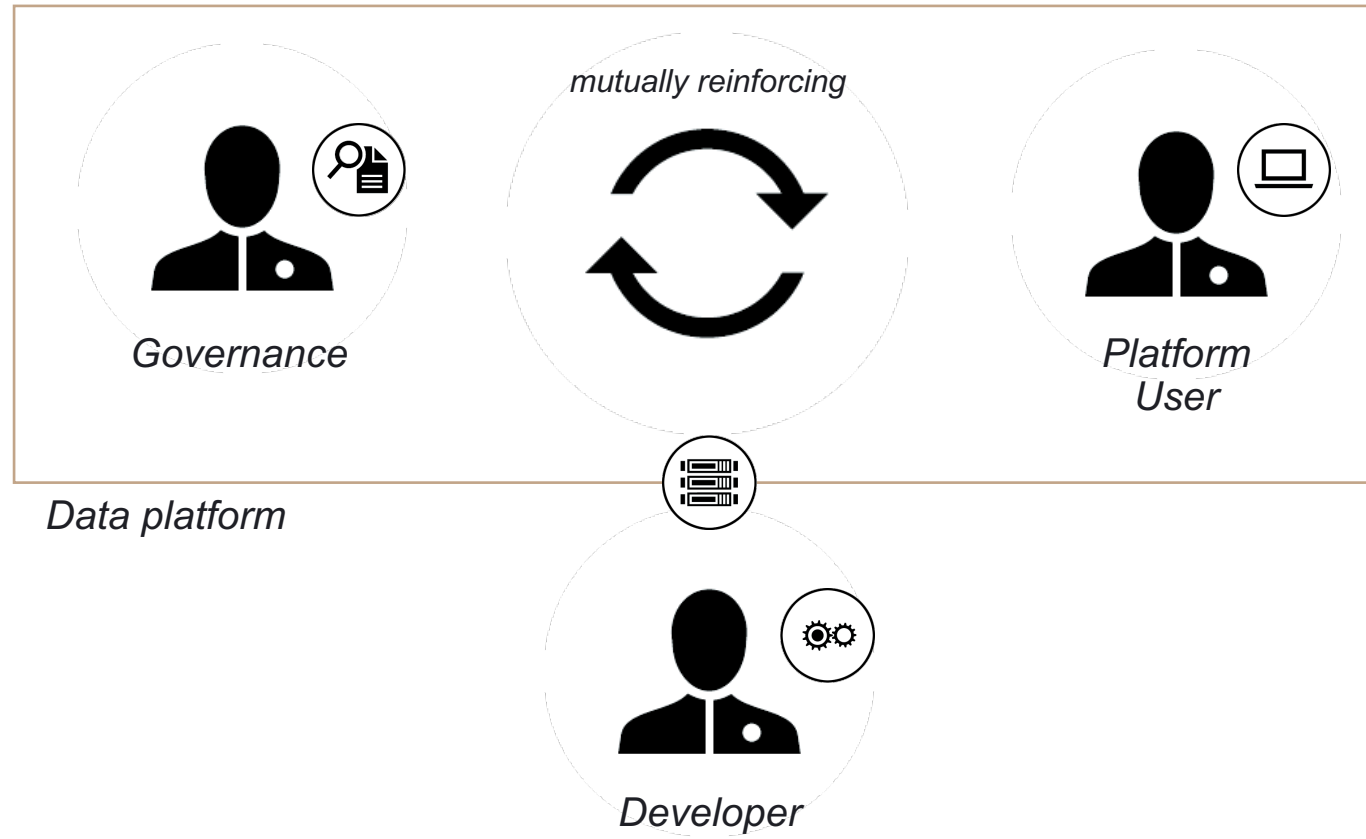
- **Simple APIs** for configuring, displaying, and reviewing justification prompts and user-submitted justifications
- Purpose Justification **Object Model**
- **Generalized Architecture** for Purpose Justification Framework

## Purpose Justification Framework Starter Kit



## Outcomes and feedback

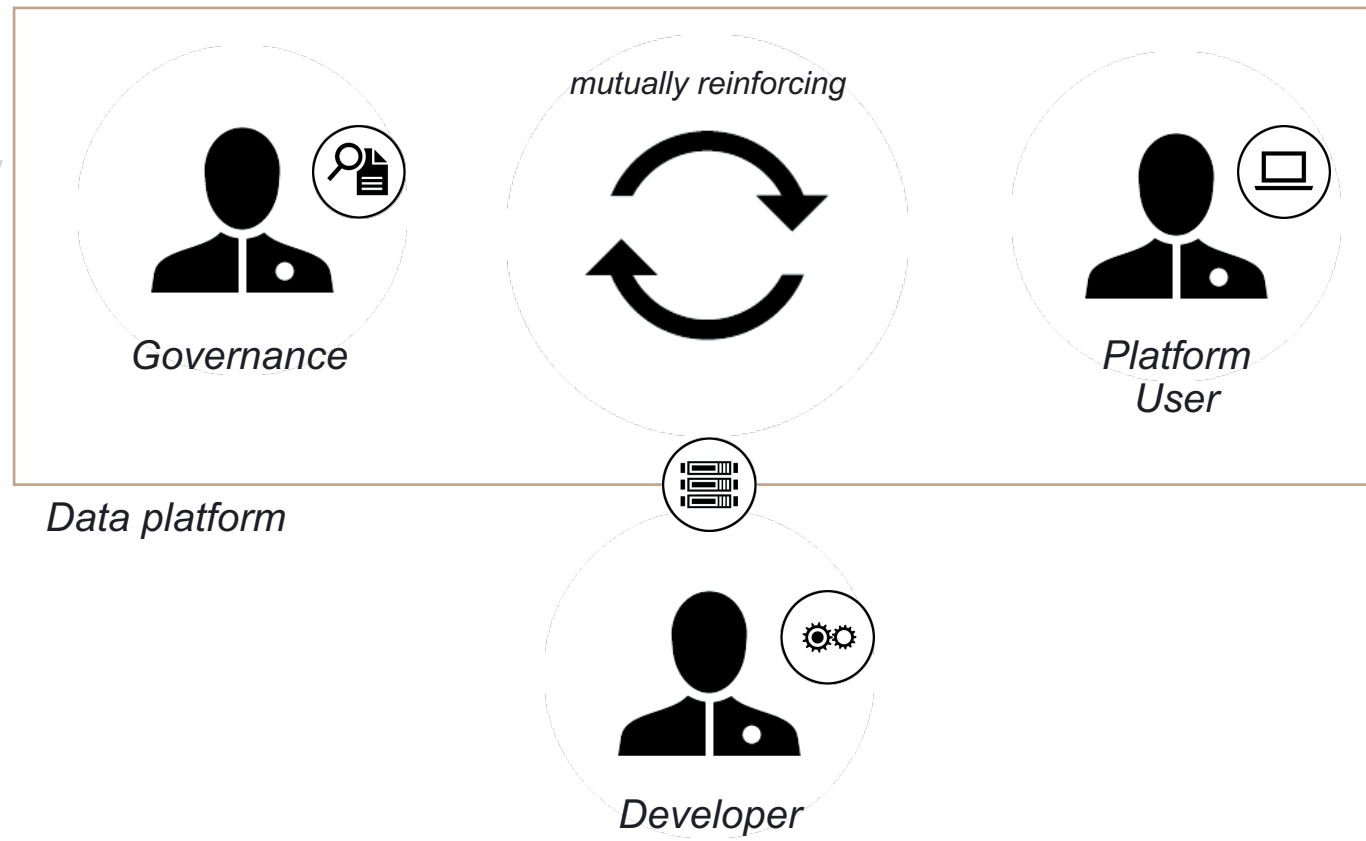
- Greater awareness and context of user activity
- Flag gaps in existing accountability procedures
- Improve processes and training over time





## Outcomes and feedback

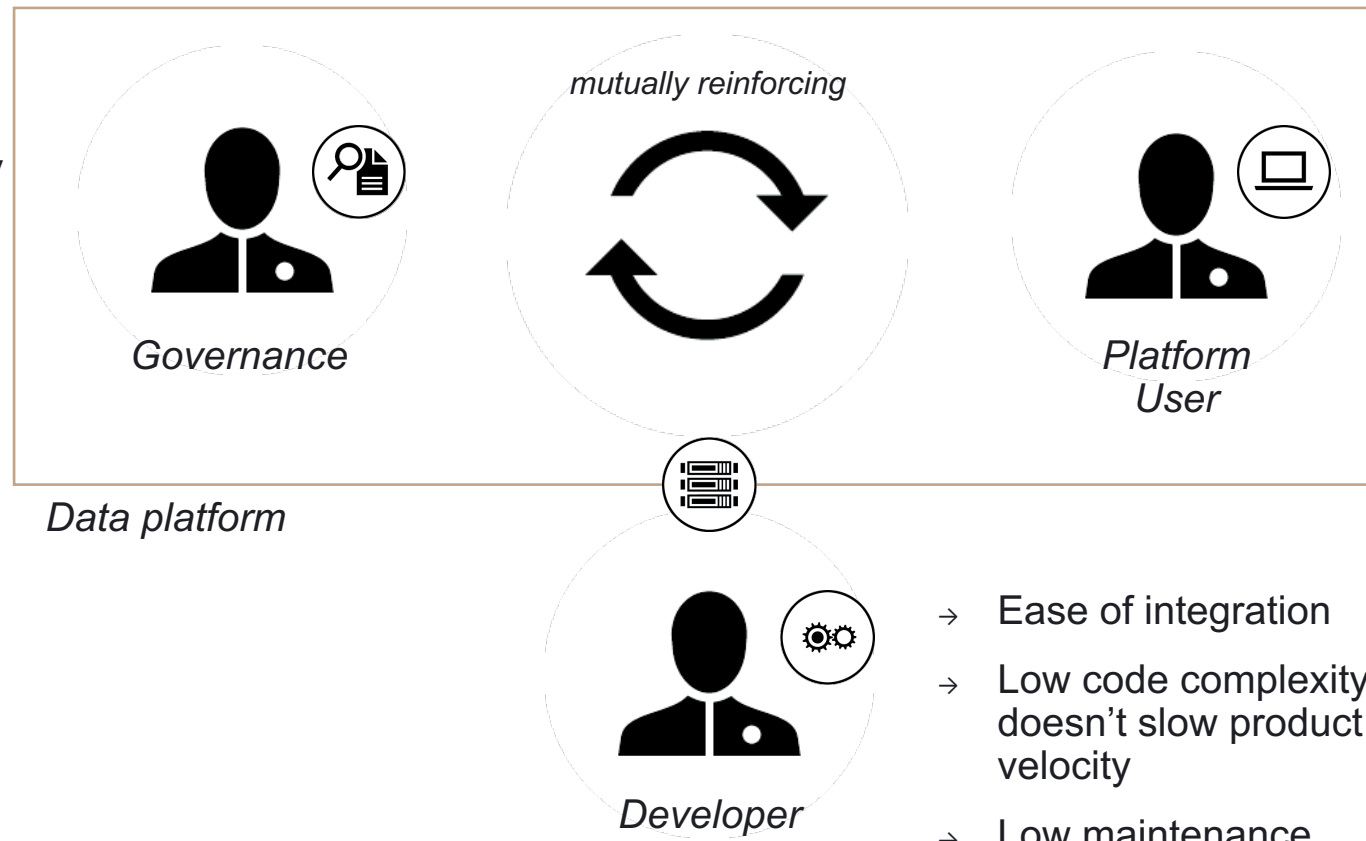
- Greater awareness and context of sensitive user activity
- Flag gaps in existing accountability procedures
- Improve processes and training over time



- 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

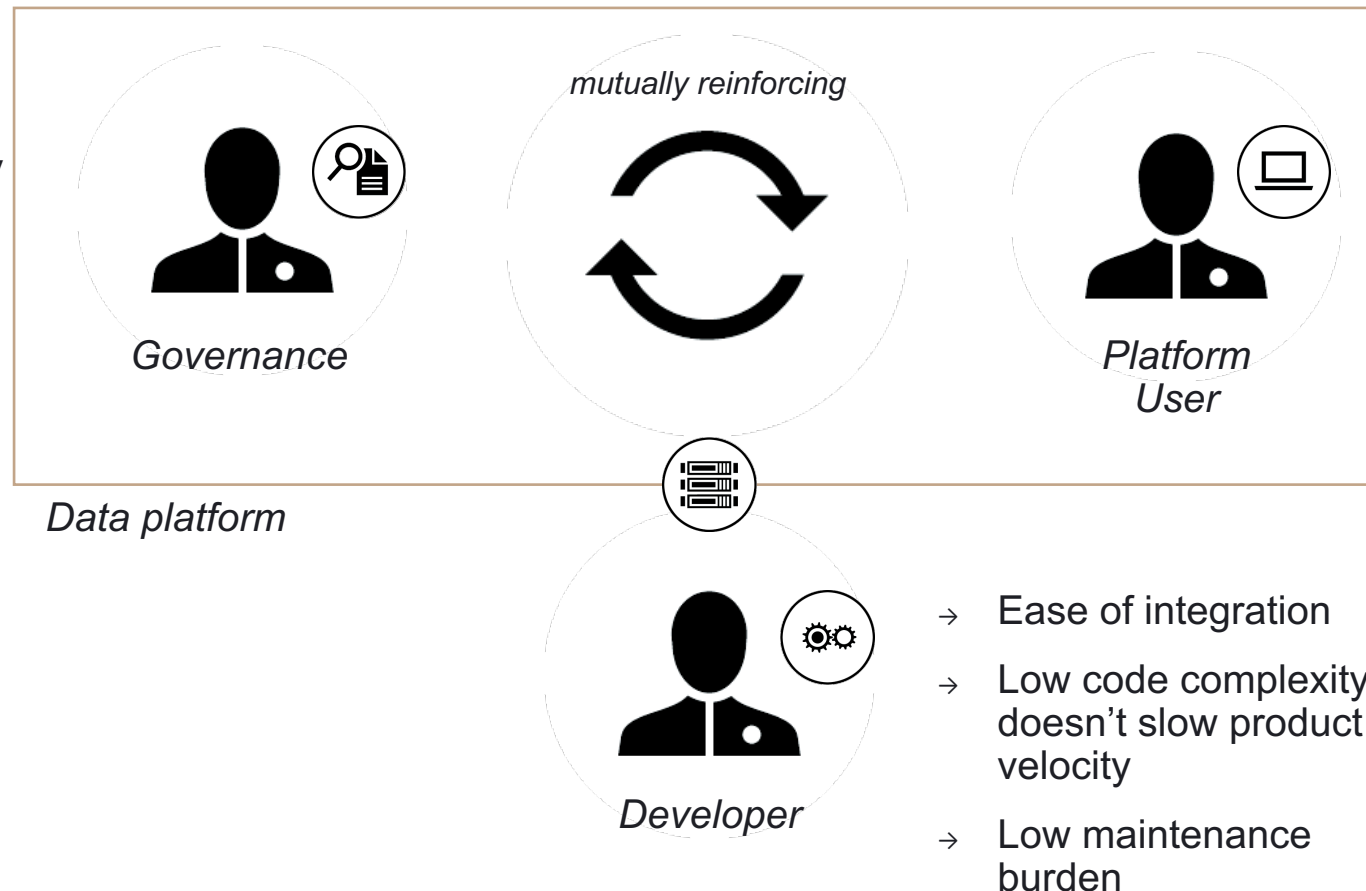


- Reminder and nudge of sensitive action
- Organizational policy at fingertips at action-time
- When unsure, have an escalation path to check

- Ease of integration
- Low code complexity doesn't slow product velocity
- Low maintenance burden

## 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

# Lightweight Purpose Justification Service for Embedded Accountability

*PEPR 2021*

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