May 2022

DYNAMIC DATA AND POLICY RELATIONSHIP TECHNOLOGIES FOR DATA PRIVACY COMPLIANCE IN ECOSYSTEM

HP INC

Dynamic Data and Policy Relationship Technologies for Data Privacy Compliance in Ecosystem

Abstract: A cloud system controls data collection from clients and devices in compliance with privacy requirements without the need for software and/or firmware changes to the clients or devices.

This disclosure relates to the field of data privacy.

A technique is disclosed that automatically adjusts the control of data collection from different clients and devices based on data privacy laws for a specific entity (i.e. country), customer consents for data collection, and joining/subscribing of different services and/or programs. The clients and devices do not require any complicated logic in deciding what to collect, but rather provide its relevant identifiers to the system which then, in turn, decides what can be collected. This data processing method is performed across the system at an atomic data element level based on the mentioned changing criteria.

There exist both business and technical problems regarding compliance with data privacy laws and requirements. Businesses need to be data privacy compliant in their data collection and use at a country/entity level. From a technology perspective, this typically requires frequent or continuous changes to software and firmware to meet the requirements, let alone determine how to maintain firmware for various forthcoming data privacy laws in a region. The failure to comply, and/or to show compliance, results in business risk and liabilities. However, becoming and remaining compliant incurs engineering and maintenance costs, which can in turn delay launches of new products and innovation.

According to the present disclosure, and as understood with reference to the Figure, the disclosed data valve system provides a dynamic data relationship architectural approach to readjusting the way data collection and use is managed, without changing firmware and software components. It systematically controls dynamic data relationships based on contextual criteria including, data privacy policy/guidelines, country/entity, user/client identities, entitlements, subscriptions, and/or program participation.

This technique for managing those data-to-policy relationships allows edge components (for example, software clients and printers/devices) to focus only on enforcing what should be collected based on the instructions from the central master valve controller. The master valve controller resolves all the contextual criteria for the edge components. If and when contextual elements change, adjustments to the necessary data collection policies for an edge component is effected in near real-time.

A Master Valve Controller (MVC) 10 resolves business logic and data privacy policies on behalf of the system. It produces a data collection manifest which uniquely describes the requirements with which the data valve must comply.

At least one Local Valve Controller (LVC) 20 controls certain edge components for which they communicate with the MVC 10 to obtain the data collection manifest for a specified edge component (or components), and to obtain the appropriate atomic attribute list. It then translates this into the specific physical layer bindings by which the collection policy can be understood by the edge component(s). In addition, when needed, the local controller will subset data if the parcel is too inclusive.

At least one Data Valve (DV) 30 enforces the data attributes collected at the edge component, and can send this data to another component external to the edge component.

A master Data Dictionary 40 of all available atomic data attributes (current and future) has the data privacy compliance relationships to a given data privacy policy for a given entity/country. The Data Dictionary 40 is created and updated per product development and data privacy governance process.

The technique operates as follows:

1. When a new edge component (for example, a printer) is registered to the cloud system, the respective LVC 20 makes a request to the MVC 10 to ascertain what data can be collected by the edge component (printer).

2. The MVC 10 takes the information sent by the LVC 20 and performs processing based on the data management criteria for the system. Using the edge component identifiers and other metadata, the MVC 10 assesses other contextual data such as consent data, country/entity data, subscriptions, programs, and entitlements. Once processed, a unique data collection manifest is generated and sent back to the LVC 20 as the response.

3. The LVC 20 then uses the data collection manifest to retrieve the specific data attributes (or its identifiers) that the edge component is permitted to collect and emit.

4. The LVC 20 then translates the list of atomic data attributes to the proper interface (physical layer) and sends it to the edge component, in some cases via the Data Valve 30 of the edge component.

5. The Data Valve 30 of the edge component enforces the data attributes to collect and emit.

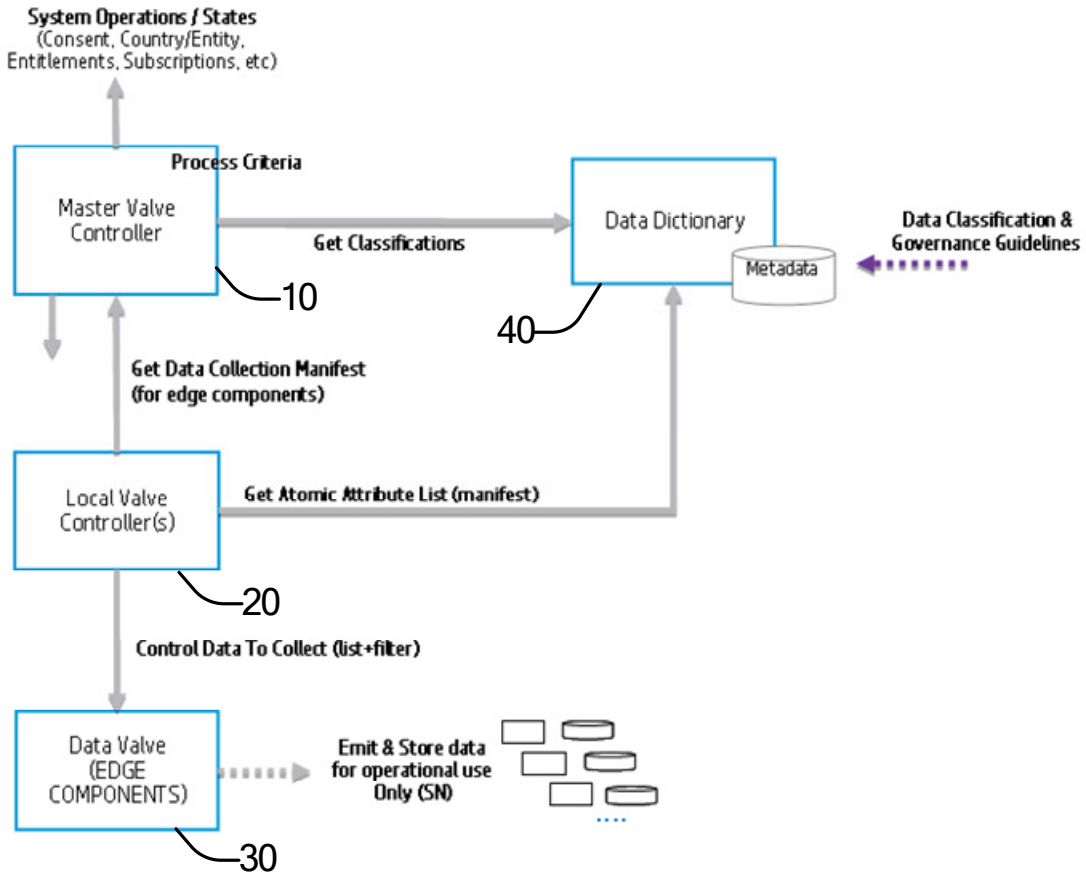
6. Based on operational needs, the data attributes (whether telemetry-based or event-based) are collected over time until the system determines that the criteria for collection have changed. Such events may include a change in consents, an add or delete of a subscription, or a change in entitlement. In such a case, the appropriate components are triggered to inform the LVC 20 and/or Data Valves 30 to update the collection policy for the Edge Component.

7. In addition, when a certain data privacy policy changes, the system generates a system policy event to which the components can register and be triggered to update the appropriate edge components on the collection profile. Such data privacy policy changes may include, for example, a change in what can be collected for a certain country.

The disclosed technique advantageously provides control of data valves by consent, country, and programs. Firmware changes are not needed to abide by changes in the data privacy guidelines. The firmware does not need to know the business logics and variances of privacy laws; this is fully abstracted away from firmware. The technique

applies to any software client and service that requires data collection. As new products are introduced, the data valve system scales to accommodate the new products without changing software throughout the system. Compliance audits can be more easily handled due to the nature of the data management and governance approach system-wide.

Disclosed by Joseph Yang, Phillip A. Mccoog, and Manjunath Bhuyar, HP Inc.


System Operations / States
(Consent, Country/Entity,
Entitlements, Subscriptions, etc)
Process Criteria
Master Valve
Controller
Get Classifications
Data Dictionary
Metadata
Data Classification &
Governance Guidelines
10
40
Get Data Collection Manifest
(for edge components)
Local Valve
Controller(s)
Get Atomic Attribute List (manifest)
20
Control Data To Collect (list+filter)
Data Valve
(EDGE
COMPONENTS)
Emit & Store data
for operational use
Only (SN)
30