SmartData Fabric® (SDF)

Multi-jurisdictional Data - Data Sovereignty Solutions

July 2022

Introduction

- Banks and other international companies need to operate across multiple countries with different data sovereignty and privacy laws, without copying or moving the data or contravening these laws
- GDPR, CCPA and similar regulations are increasingly in-place and being enforced
- As per reference 1,"**the lack of regulatory and data standardization is continuing to cause issues with implementing a best practice approach to compliance**."

Drivers for international companies

Consolidated data is needed to run international companies, to:

- Understand and manage risk
- Monitor and operate the business
- Report to regulatory authorities and shareholders

Constraints facing international companies

1. **Personal data cannot be accessed from outside a specific jurisdiction**, the rules of which are defined by the jurisdiction itself, e.g., local, region within a country, country, region of countries or global organization
2. **Personal data stored within a jurisdiction may be accessed by individuals within the jurisdiction** who have the required user credentials, as determined by data governance, access control and data security
3. **Personal data and associated transaction data accessed from outside a jurisdiction must be anonymized and aggregated** to prevent any risk of identifying individuals within a jurisdiction - this makes processes such as KYC and single customer views across jurisdictions extremely difficult, if not, impossible
4. **Personal data may also be subject to GDPR and similar personal data privacy regulations** within a jurisdiction and/or a higher-level jurisdiction, e.g., a region

Characteristics of a Secure Data Mesh

- **Data mesh is not a technology**, but is instead a data fabric with a shift in responsibility and accountability for data placed on data owners, instead of a central organization department
- **Data mesh empowers data owners** to both comply with jurisdiction laws and policies, and ensure that their data is secure and, in some cases, anonymized for consumption by various "customers" within and external to a jurisdiction
- **Data can be accessed in various ways**, including APIs
- **Data first needs to be pre-processed without impacting operations**, i.e., discovered, identified, secured, cleansed, transformed, standardized, governed, normalized, integrated, access controlled, and available for query processing

SmartData Fabric® uniquely enables capabilities of a Secure Data Mesh to meet the demanding requirements of multi-jurisdictional data solutions

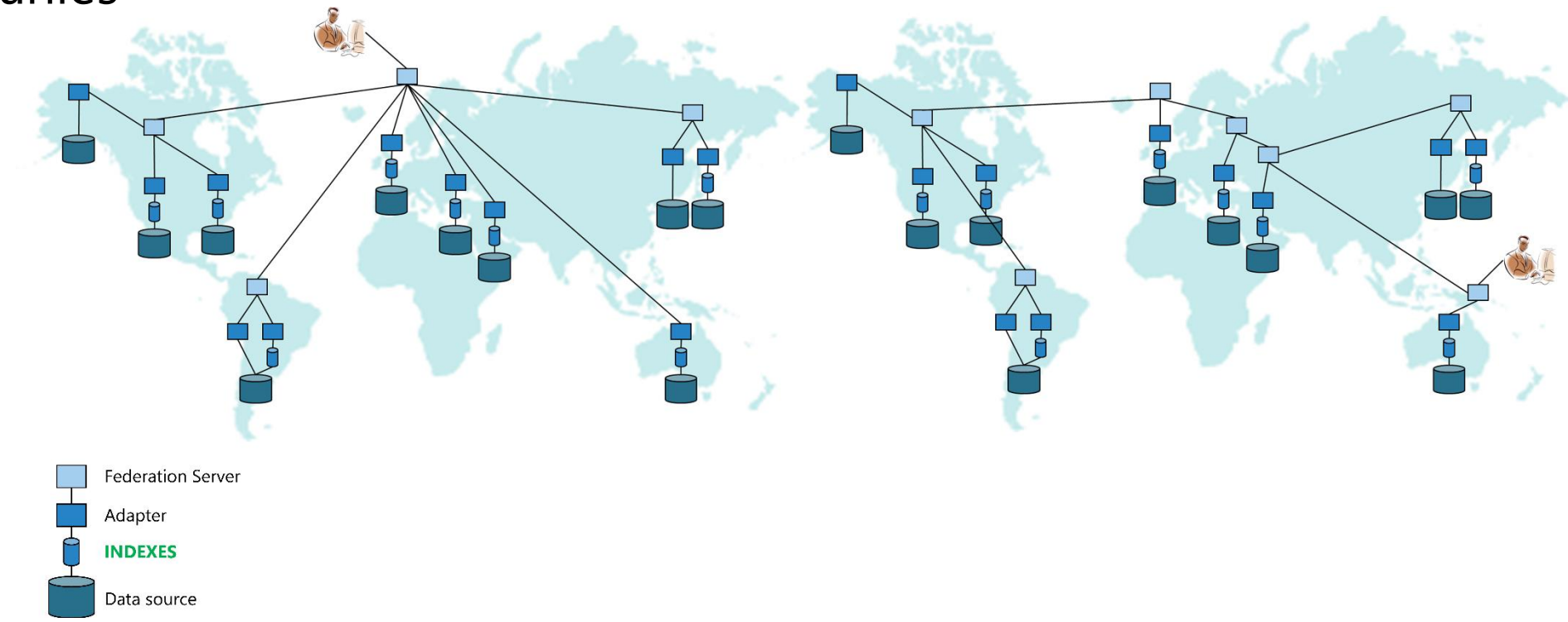
General data security and privacy protection considerations

- Each jurisdiction will have its own laws and policies as they relate to data and access to it, and these fall into general categories:
  - Data handling within and across jurisdiction domains – storage, transit and use
  - Data access – roles and users, associated data elements and read/write privileges
  - Permissions/consent – specific records of users/entities that have associated permissions/consent and rules/forms for sharing, etc. - some of these may be from an individual customer preference as allowed under GDPR and similar regulations
  - Masked/anonymized data
  - Tokenized data, also tokenized encryption
  - Substituted data
  - Approximation or broad range for data
  - Aggregated data – specify minimum number of participants and caps on contributed records per jurisdiction, customers, etc., similar to Safe Harbor info sharing regulations in the US

Secure data mesh using SmartData Fabric®

Allows both:

- **Stringent local controls** that enforce jurisdictional laws and policies, and
- **Global consolidation/aggregation** of anonymized data for international companies



Drivers for international companies

Global consolidated data is needed to understand and manage risk, monitor and operate the business, and report to regulatory authorities and shareholders

SmartData Fabric®

- Supports "live query" mode in addition to the more common "data extract" mode of most reporting, BI and analytics tools, e.g., Power BI and Tableau, that copy data from sources to a centralized store for complex query processing. In live query mode, these tools execute complex queries on the source indexes and adapters and then consolidate results from multiple sources and/or jurisdictions
- Is one of the few (if not the only) data virtualization/fabric/mesh tool that supports federated queries from reporting, BI and analytics tools
- Is the only data virtualization/fabric/mesh tool that can support uniform SQL query processing on standard indexes and adapters, with no need to modify queries to fit specific data sources or accommodate issues with data sources
- Honors local data source and jurisdictional laws and polices before (a) a query is made on specific sources, (b) any data is read and used in a specific data source result-set, and (c) results data is read and consolidated subject to review for Safe Harbor and similar jurisdictional laws and policies
- Allows local data source policies and jurisdiction laws and policies to prevail over global laws and policies

Constraint #1 facing international companies

Personal data cannot be accessed from outside a specific jurisdiction, the rules of which are defined by the jurisdiction itself, e.g., local, region within a country, country, region of countries or global organization

SmartData Fabric®

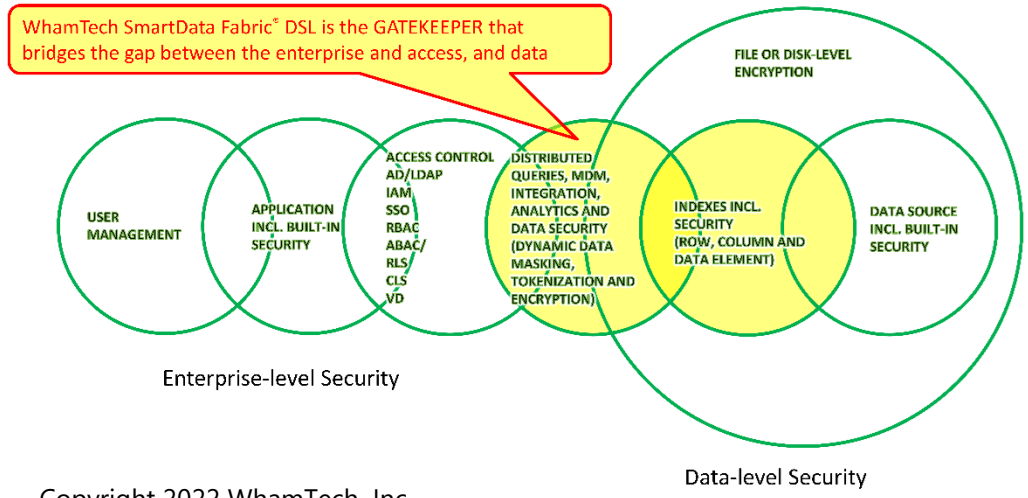
- Leaves data stored and updated in sources, whether that be the original source or a copy in a local data lake (or both)
- Indexes only data and/or data sources that need it - much/most data may not, e.g., transaction data, and associates source-specific indexes and adapters to:
  - Discover, identify, classify, secure, cleanse, transform, standardize and connect data
  - Generate/use, and seamlessly and automatically integrate master data, e.g., essential for KYC
  - Present multiple standardized views of data, including APIs, aggregations, joins, calculations and virtual graph database
  - Execute uniform SQL queries from standard apps across all federated adapters to yield pointers to raw results data in sources
  - Use pointers to read, and then transform, standardize and secure, raw results data from sources
  - Provide integrated clean, standardized, secure, accurate and complete results data to standard apps at multiple levels

Constraint #2 facing international companies

Personal data stored within a jurisdiction may be accessed by individuals within the jurisdiction who have the required user credentials, as determined by data governance, access control and data security

SmartData Fabric®

- Is a data catalog that standardizes views of source data that can then be used for data governance
- Rigidly applies local domain-specific data source access control, data governance and data security depending on local roles and user credentials and permissions
- Can enforce external-to-jurisdiction data governance, access control and data security in several ways, including passing through specific users or user proxies, depending on jurisdiction and global organization laws and policies – jurisdiction laws and policies and local data source policies will always prevail



Constraint #3 facing international companies

Personal data and associated transaction data accessed from outside a jurisdiction must be anonymized and aggregated to prevent any risk of identifying individuals within a jurisdiction - this makes processes such as KYC and single customer views across jurisdictions extremely difficult, if not, impossible

SmartData Fabric®

- Applies dynamic data masking, tokenization, encryption and anonymization to results data depending on local roles and user credentials and permissions, which would stem from jurisdiction and global organization laws and policies
- Restricts results according to jurisdiction and global organization laws and policies – these may involve pruning or returning no results because of these laws and policies

Constraint #4 facing international companies

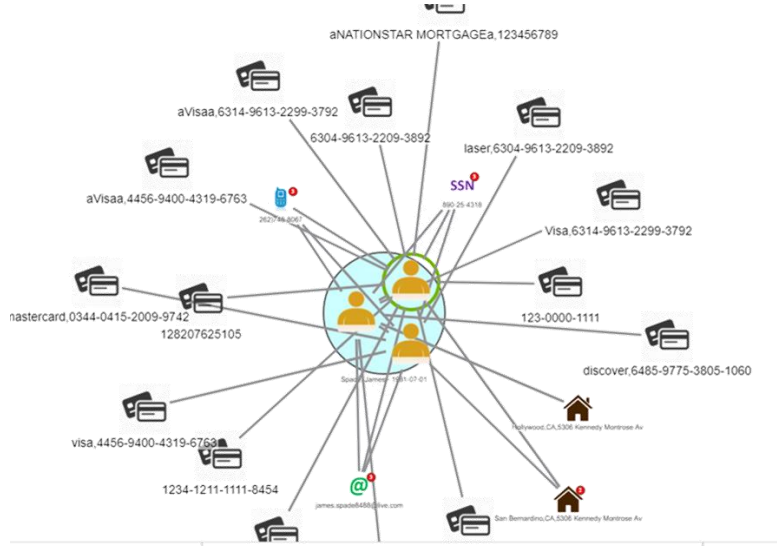
Personal data may also be subject to GDPR and similar personal data privacy regulations within a jurisdiction and/or a higher-level jurisdiction, e.g., a region

SmartData Fabric®

- Supports being able to keep track of personal data, but also a customer's wishes on how that data is used because it can simultaneously track and represent logical virtual views of data and physical storage
- Allows MDM to take place at multiple levels, within and across multiple data sources and potentially multiple jurisdictions, subject to the jurisdiction and global organization laws and policies

LOGICAL VIEW

PHYSICAL VIEW



SmartData Fabric® uniquely enables capabilities of a Secure Data Mesh to meet the demanding requirements of multi-jurisdictional data solutions, by
(a) supporting the drivers to run international companies, and
(b) addressing the constraints imposed by individual jurisdictions

References

1. https://www.finextra.com/blogposting/11331/the-challenges-of-multijurisdictional-regulatory-compliance-and-entity-data-management, Fenergo, June 22, 2015 [aged, but still applies]

The End