2.3.4.6 Geographic Jurisiction Data Governance

Return to Data Taxonomy

Overview

Return to Top

> *Geographic Jurisiction Data Governance is the judicial (legal and contractual/policy) considerations that are applicable within and across physical geographic boundaries/areas.* [1)]

Originally, before the ubiquitious use of neworks and internet, hardware abstraction, virtualization, the explosion in cloud computing, and globalizaton of tech compaines, data protection was relatively easy which a large portion of the Data Protection accomplished through Physical Security. Thess original concepts of Data Protection were greatly expanded to cover Securability. Although, this was an improvement in protecting data from the perspective of the corporation, there was little protection for the end-user (i.e., consumer) from the corporations. Figure 1 represents the widespread nature of Geographic Jurisiction Data Governance. Fortunately, most of the tecg areas such as Cloud Computing, Artifical Inteligence and Big Data have already made adaptations for Geographic Jurisiction Data Governance expecially since it has been mandated by Internation and national Governance and Regulation such as General Data Protection Regulation (GDPR), Data Protection Act 2018, and California Consumer Privacy Act (CCPA).

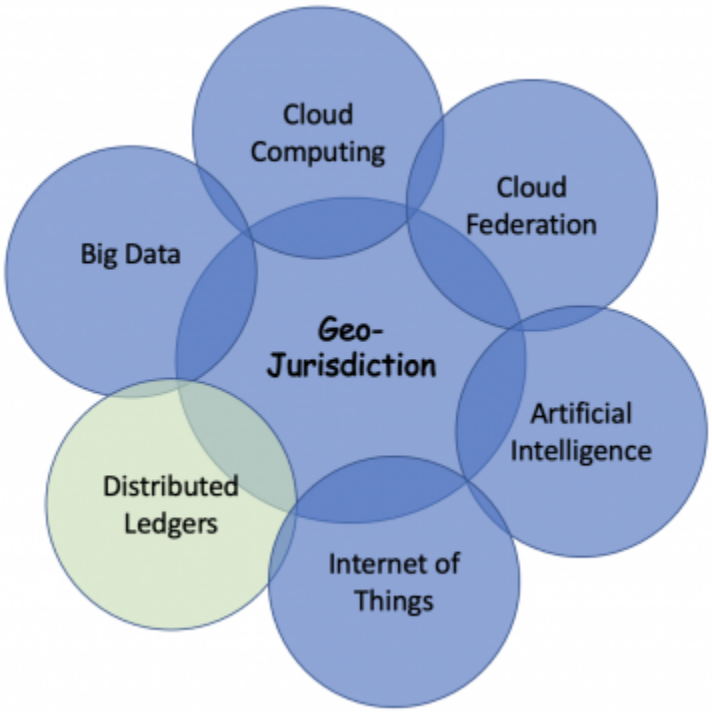

Figure 1: Geographic Jurisiction Data Governance touches most technical areas see [2)]

Unfortunately, most distributed computing platforms (i.e., DIDOs) have done little to address Geographic Jurisiction Data Governance even while the amount of governance and regulation has increased beome relatively mainstream internationally. Some of the Countries that have enacted data protection laws are https://incountry.com/country-compliance/, https://incountry.com/blog/data-residency-laws-by-country-overview/:

- China
- Russia
- India
- Indonesia
- Saudi Arabia
- Switzerland
- Turkey
- United Arab Emerites
- United States of America
- State of California

Kinds of Geographic Jurisiction

Return to Top

There are three main categories of Geographic Jurisiction Data Governance: data_residency, Data Sovereignty and Data Localization. Usually, these concpets are applied strickly to data storage with an increase burden to store the data in the jurisdiction where the data is created. Basically, it is represents the Data-at-Rest data state, see: 2.3.4.2 State of Data Taxonomy.

Data Residency

Return to Top

> ***Data Residency*** *refers to where a business, industry body or government specifies that their data is stored in a geographical location of their choice, usually for regulatory or policy reasons.*
>
> *A typical example of a Data Residency requirement in action is where a company wishes to take advantage of a better tax regime. Doing so will usually require the business to prove they are not conducting too great a proportion of core business activities outside that country's borders – including the processing of data. They will therefore impose a Data Residency that requires them to use certain infrastructures, and then impose strict data management workflows on themselves and any cloud service providers in order to protect their taxation rights.*[3)]

Data Sovereignty

Return to Top

Data Sovereignty *differs from Data Residency in that not only is the data stored in a designated location, but is also subject to the laws of the country in which it is physically stored. This difference is crucial, as data subjects (any person whose personal data is being collected, held or processed) will have different privacy and security protections according to where the data centers housing their data physically sit.*

This difference is also crucial for businesses, as a government's rights of access to data found within its borders differ widely from country to country. This is where data sovereignty and residency are often conflated. Ensuring data sits within a geographical location for whatever reason - whether avoiding or taking advantage of laws, regulations and tax regimes, or even for pure preference and comfort - is a matter of Data Residency. But the principle that the data is subject to the legal protections and punishments of that country is a matter of data sovereignty.

They are clearly related, and even two sides of the same coin, but one is a matter of national legal rights and obligations, while the other is a matter of geography. Recognizing this distinction will help professionals better prepare for compliant data management and exchange.[4)]

Data Localization

Return to Top

Data Localization *is the most stringent and restrictive concept of the three, and like data sovereignty, is a version of Data Residency predicated on legal obligations. It is also the concept that is growing the fastest internationally.*

Data Localization requires that data created within certain borders stay within them. In contrast to the two terms above, it is almost always applied to the creation and storage of personal data, with exceptions including some countries' regulations over tax, accounting and gambling.

In many cases, Data Localization laws simply require that a copy of such data be held within the country's borders, usually to guarantee that the relevant government can audit data on its own citizens (provided there is due cause) without having to contend with another government's privacy laws. India's draft Personal Data Protection Bill is an example of exactly this (you can see more discussion of the Bill in our Director of Data Privacy Services' blog here).

However, there are countries where the law is so strict as to prevent it crossing the border at all. For instance, Russia's On Personal Data Law (OPD-Law) requires the storage, update and retrieval of data on its citizens to be limited to data center resources within the Russian Federation.[5)]

Geographic Jurisiction Concerns

Return to Top

The main empasis of Julian Box's article is on Cloud Computing[6], however, many of the concerns and issues he raises are pertenant to Distributed Compuing since the data within the distributed solution potentially can reside anywhere, especially with a Permissionless Network.

He suggests as a starting point for Cloud Computing, try applying the distinctions between data_residency, Data Sovereignty and Data Localization to the following questions about your distributed system:

- When In-Motion, which jurisdictions does your data pass through?
- When In-Use, which jurisdictions have access to the distributed data. In other words, where are the Consensus Algorthims run?
- When At-Rest:
    - Where are each of your various categories of data (personal data, financial records, etc) created or processed and what obligations might this bring?
    - Where is it then stored, and who owns the data center? Your data may be in a data center in the UK, but if this data center is owned by a US-headquartered company, then the US Government may have the rights to access your data under the CLOUD Act.
    - What are your procedures for back-up? Where is your data backed up to? According to the type of data in question, what local stipulations exist for the security or encryption of that data?
    - How confident are you in your cloud partner(s) understanding of current and future data privacy regulations? How have they evidenced that their data centers meet all your local and global privacy needs, or have you assumed it?

[1] [2]

Steven Woodward, Geo-Jurisdictions: Myths, Realities and Complexities, Cutter Business Technology Journal, Vol 31, No. 8, 2018, The Critical Need for Data Governance, https://www.cutter.com/article/geo-jurisdictions-myths-realities-complexities-500906

[3] [4] [5] [6]

Jullian Box, Data Sovereignty vs Data Residency vs Data Localization, 12 March 2019, Accessed: 6 October 2021, https://www.insightsforprofessionals.com/it/storage/data-sovereignty-data-residency-data-localization

From:
https://www.omgwiki.org/dido/ - **DIDO Wiki**

Permanent link:
https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:1.2_views:3_taxonomic:4_data_tax:06_protect:start&rev=1633546345

Last update: **2021/10/06 14:52**