CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

Cloud Governance Project
Security and Robustness

Localization and Routing Requirements

Governments and customers are increasingly concerned with where their data is stored and processed, as well as the jurisdictions through which it travels. To secure their citizens' data against interception and to use it for their own national security, law enforcement, or economic objectives, many governments are creating new data-localization[1] and routing requirements.[2] Yet these measures also have negative side effects, contributing to the "fragmentation" of the cloud and reducing its efficiency, increasing the costs and/or decreasing the utility of cloud services, and undermining their availability and functionality.

Key Considerations

- ***Large number of stakeholders complicate routing security efforts.*** Cloud providers do not move data alone. This process also involves internet service providers and other content delivery networks (CDN). The number of involved parties complicates efforts to secure routing, including determining if the routed data originates from and is announced by a legitimate source, and using egress filters to prevent malicious traffic from transiting the network.
- ***Cloud fragmentation***. Data localization and routing requirements may lead to isolated cloud environments in countries or regions around the world, contributing to the risk of a "fragmented" cloud, which may adversely affect service availability and functionality for cloud customers and limiting cloud network redundancy. Cross-border transfer arrangements can potentially remedy this issue.
- ***Overbroad mandates and increased compliance costs***. A shortage of technical expertise in government may lead to overbroad localization mandates that fail to distinguish between different types of data (personal, sensitive, operational, and so on). Such mandates run the risk of increasing compliance costs for cloud providers and enterprise customers.
- ***Regulatory burden.*** Ill-defined or conflicting data localization and routing requirements can create legal[3] and operational issues for providers, potentially reducing the efficiency of cloud services.

Stakeholder Perspectives

Government	Cloud Providers	Customers	Others
• Are inclined to see data localization	• Are wary of localization	• Seek robust protections against	• N/A

requirements as serving multiple purposes, such as enhancing privacy protections for citizens' and commercially sensitive data, and supporting their local economy. They may also see it as a way to secure for themselves better and more reliable access to cloud-hosted data.

- May wish to set requirements that providers not route traffic through certain jurisdictions (or alternatively, *only* route traffic through certain jurisdictions) in order to avoid the interception of cloud data by unfriendly entities as it crosses borders.[4]
- May wish to protect and grow the domestic cloud services market by using data localization requirements to raise the costs foreign providers face when operating domestically.

mandates and routing requirements that may negatively impact operations, security, customer trust and privacy, and business presence in foreign countries.

- May be skeptical of government security concerns and the possibility of interception of data flows, and thus have an interest in maintaining as much freedom as possible in routing operations for functionality and security.
- Are wary of excessive prohibitions on exporting data and services.

unauthorized access and invasion of privacy, which may occur through localization and routing requirements.

- *Enterprise Customers*: Wish to retain the ability to move and keep data where they want it securely.[5]

Tensions with Other Cloud Governance Issues

- ***Security and Privacy in Lawful Government Access***: Data localization requirements may offer governments new opportunities to access cloud-hosted data
- ***Cloud Access Restrictions and Content Moderation***: Data localization requirements may enable or facilitate additional steps in censoring or surveilling a population.
- ***Equitable Cloud Access***: Data localization requirements can increase the cost of cloud services in those jurisdictions if compliance with them involves the creation of new, expensive cloud infrastructure. This could make cloud services less affordable to lower-income populations in those regions.
- ***Effects of Cloud Market Concentration***: Government restrictions on data movement may raise costs for businesses seeking to enter new markets or expand innovative products and services to other countries.
- ***Environmental, Community, and Energy Market Impact***: Data localization requirements may increase cloud providers' carbon footprint by requiring that they build new resource-intensive datacenters. Operating these may involve greater financial and environmental costs given operational and technical considerations.

Potential Ways Ahead

Government

- Narrowly target localization requirements (for example, by type of data, level of sensitivity, and so on).
- When drafting cross-border transfer arrangements, include measures to preserve confidentiality of data, both in terms of legal prohibitions against unlawful access and in terms of security provisions.

Providers

- Work with governments to understand distributed processes of data routing and work with other stakeholders to increase confidence in the security of data in transit. (Shared with Governments and Customers.)
- Educate concerned parties on the distributed process of data routing and its role in cloud service

Customers

- Work with providers to understand distributed processes of data routing and work with other stakeholders to increase confidence in the security of data in transit. (Shared with Governments and Cloud Providers.)

Others

- N/A

- Work with providers to understand the distributed processes of data routing and work with other stakeholders to increase confidence in the security of data in transit. (Shared with Cloud Providers and Customers.)
- Work with foreign governments to establish international agreements and mechanisms to resolve conflicts of laws that secure sensitive data without impinging on the privacy of citizens, national security, and defense. functionality and resilience.
- Work with governments to jointly develop reference designs and technical artifacts[6] to better demonstrate how the cloud provides for data security at rest and in motion. (Shared with Governments.)
- Commit to and encourage the adoption of actions that enhance routing security.[7]

Recent Examples and Additional Resources

- European Safe Harbor Convention ‘s invalidation by the Schrems case, 2020. For additional information, see: “The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield,” Court of Justice of the European Union, July 16, 2020.
- India, Vietnam and Indonesia struggle to implement data localization mandates, 2020. For additional information, see: “The Retreat of the Data Localization Brigade: India, Indonesia and Vietnam,” The Diplomat, January 10, 2020.
- Google internet traffic was mistakenly routed through China, Russia, and elsewhere, 2018. For additional information, see: “Google Internet Traffic Wasn’t Hijacked, But It Was Out of Control,” *Wired*, November 13, 2018.

Notes

[1] Data localization requirements, which mandate that data stay in a particular jurisdiction, or that a copy of all data be maintained in the jurisdiction at all times, often require the construction of expensive and potentially redundant cloud-infrastructure.

[2] Governments and customers may have concerns over the routing of their traffic through potentially hostile or otherwise unsafe territories, worrying that their data may be vulnerable to interception, destruction, and even manipulation while transiting such jurisdictions. These requirements may force providers to route data in less-optimal network pathways, deviating from their practice of making routing decisions to optimize the speed and efficiency of services.

[3] For example, being required to facilitate government access to data under one country's laws and being prohibited from doing so under another's.

[4] See: Barton Gellman and Ashkan Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say," *The Washington Post*, October 30, 2013, https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

[5] The localization of data in-territory does not guarantee its security. Data security is attained through encryption and robust zero-trust system architectures.

[6] See: IBM, "Network security architecture," IBM, n.d., https://www.ibm.com/cloud/architecture/architectures/network-security-arch and Ciara Gallager, "Data in motion – how to protect it – 5 Key Considerations," Microsoft Pulse, n.d., https://pulse.microsoft.com/en-ie/technology-lifestyle-en-ie/na/fa3-data-in-motion-how-to-protect-it-5-key-considerations/.

[7] The Internet Society's "Mutually Agreed Norms for Routing Security (MANRS)," whose members include Akamai, AWS, Cloudflare, Google, and Microsoft (among other key stakeholders, such as internet service providers), sets out 6 security-enhancing actions for cloud providers and Content Delivery Networks. These include: (1) ensuring the correctness of routing announcements issued by their peers and customers (this can be achieved through explicit ingress filtering, using RPKI and IRR as validation protocols) and whenever possible, checking that the announcements originate from legitimate sources; (2) implementing anti-spoofing controls to prevent traffic with illegitimate source addresses from leaving the network (aka, egress filtering). This will require monitoring and controlling what their customers, who are using virtual machines, can do on the network; (3) registering routing information in public routing repositories (e.g., IRRs and RPKI). Doing so will motivate third parties to do the same, which will enable other network operators to validate routing announcements on a global scale; and (4) offering routing monitoring and debugging tools to peers and if possible, to the

wider public. See: MNRS, “MANRS for CDN and Cloud Providers,” MANRS, March 1, 2021, https://www.manrs.org/cdn-cloud-providers/.