CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

Cloud Governance Project
Stakeholders

Government

Below are measures legislators and regulators can take to make progress on individual cloud governance issues.

Security & Robustness

Cloud Certification and Auditing

- Improve communications channels between government and industry to provide feedback on and refine existing certifications processes by identifying areas in need of adjustment. These include a clear delineation of roles and responsibilities among auditing entities, irregularities in risk assessment, and validation across authorizers. (Shared with cloud providers.)
- Work with cloud providers and enterprise customers to define high-level performance-based requirements and metrics for confidentiality, integrity, and availability of cloud services. These can differ based on the types of cloud service offered (such as storage and virtualization) and sectoral criticality. (Shared with cloud providers and enterprise customers.)
- Distinguish between requirements for less and more sensitive government workloads and align certification criteria with those requirements.
- Make audits of performance and compliance public or mandate provider's transparency on performance.

Incident Handling Procedures

- Establish mandatory standards for reporting cloud vulnerabilities and incidents that may affect systems critical to the cloud provider and/or society more broadly. These should enable close-to-real-time situational awareness for all concerned entities.
- Use governmental cloud procurement as leverage to promote cloud services security and robustness and incentivize incident reporting.
- Clarify expectations and set guardrails for incident response by government, providers, and customers (for example, hack-back, paying ransoms, degree of government access) to help establish a whole-of-system cyber risk management plan.
- Work with cloud providers, customers, insurers, and other key stakeholders to determine appropriate constituencies, documentation, and timelines[1] for disclosures. (Shared with cloud providers, enterprise customers, insurers, and credit rating agencies.)

- Consider creating a centralized incident response and reporting office for cloud sector (in consultation with providers and customers).[2]
- Facilitate cross-agency and cross-industry incident response exercises. (Shared with cloud providers and customers.)

Localization and Routing Requirements

- Narrowly target localization requirements (for example, by type of data and level of sensitivity).
- 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.
- 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.

Security and Privacy in Lawful Government Access

- Wherever possible, direct access requests to customers rather than to cloud providers.
- Allow cloud providers to notify enterprise customers in advance of government access to their data, other than in exceptional circumstances, for example by limiting the use of secrecy orders.[3]
- Mandate scoping, oversight, and transparency on government access requests (including requests received from foreign governments).
- Work with foreign governments to establish international agreements and mechanisms to resolve conflicts of laws and to ensure that foreign government access to data does not impinge on privacy of citizens, national security, and defense.[4]

Resilience

Data Retrievability and Back-up Arrangements

- Encourage diversity in routing[5] through additional geographies and geo-redundant deployments (for example, through stringent re-routing requirements and residency requirements).
- Leverage existing encryption protocols and standards for data in transit as baselines.

Government Intervention in Extremis

- Establish working groups between governments, providers, and enterprise customers to delineate clear “disaster level” thresholds necessary to trigger government intervention

as well as the process by which such intervention takes place and the circumstances under which it would conclude. (Shared with cloud providers and enterprise customers.)
- Create accountability mechanisms whereby providers and customers may ensure that governments do not overstep or abuse their intervention mandate.
- Create intervention requirements and established agreements among governments, providers, insurers, and other stakeholders to allocate liabilities and responsibilities in the event of intervention.
- Coordinate agency roles in the event of intervention.
- Increase cooperation with providers and enterprise customers by mandating joint preparedness exercises. (Shared with cloud providers and enterprise customers.)
- Coordinate with foreign governments and the appropriate cloud providers or enterprise customers to ensure that citizen privacy, national security, and defense are not at risk of compromise in the event of takeover.

Insurance for Cloud Services

- Facilitate dialogue between government, providers, customers, insurers, and other stakeholders in order to determine and clearly assign liability for cloud service disruptions (including those arising from a sophisticated attack by a nation-state). (Shared with cloud providers, enterprise customers, and insurers.)
- Develop backstopping mechanisms for cloud insurance and cyber insurance markets by drawing on backstopping in other contexts.[6]
- Define conditions for backstopping support to become available (such as the nature and/or scale of the cloud incident). (Shared with cloud providers, enterprise customers, and insurers.)
- Explore other public-private partnerships for mitigating cloud risks.
- Set requirements for cloud providers to ensure data retrievability and bolster the possibility of service continuity in the event of cloud provider or insurer insolvency.

Portability and Interoperability

- Encourage the use of hybrid and multi-cloud strategies to decrease disruption risks.[7]
- Encourage agreement on common terminology and principles for portability and interoperability in consultation with providers and customers. Definitions for these terms have been formalized in standards, including SWIPO's Codes of Conduct,[8] IEEE's P2301/P2302,[9] and ISO/IEC's 19941.[10]

Consumer & Enterprise Protection

Commercialization of Customer Data

- Establish rules requiring cloud providers and enterprise customers to publish their standard policies and practices for commercializing metadata and other anonymized usage data.

- May condition commercialization of customer data on the data subjects' consent or other bases consistent with prevailing law.[11]
- Commission studies on best practices for assessing the value of consumer and enterprise-derived data to guide policies on commercial usage and financial compensation (in consultation with providers and customers).

Effects of Cloud Market Concentration

- Promote interoperability and portability standards and multi-cloud arrangements.
- Use existing antitrust investigative and enforcement powers, including merger review and enforcement.
- Monitor and analyze evolving cloud services markets to understand when and how they might trigger competition policy concerns.
- Work with industry to develop and publish nonbinding standards for liability allocation, fairness in contracting, pricing, and so on.

Prosperity & Sustainability

Environmental, Community, and Energy Market Impact

- Support providers' efforts to substantially reduce carbon emissions or achieve "net zero" including by easing barriers to development of their own utility-scale renewable energy generation. For example, by offering financial support and/or providing liability waivers for constructing dedicated utility-scale electricity generation projects on "brownfield" sites.[12] (Shared with cloud providers and utility companies.)
- Migrate government operations to more energy efficient and sustainably powered IT infrastructure.
- Incentivize cloud providers to implement energy efficient measures, such as more sustainable server cooling methods.[13]
- Develop guidance material on best practices for reducing water usage in data centers.[14]
- Facilitate international sharing of best practices for opening local energy markets to "energy choice" programs.[15]
- Understand and mitigate the adverse impact of cloud infrastructure creation and operation on local communities. (Shared with cloud providers.)
- Creation of mechanisms to incentivize emissions reduction by, for example, incorporating new requirements into licenses and offering financial incentives.
- Integrate carbon reduction into procurement policies.
- Create consultation requirements with local communities and evaluate existing adjudication mechanisms. (Shared with cloud providers.)

Human & Civil Rights

Cloud Access Restrictions and Content Moderation

- Clearly define criteria, standards, and procedures for requiring cloud providers to take down content or deny/suspend service(s).
- Establish mechanisms to audit for bias the content moderation technologies being deployed or offered by cloud providers.
- Establish clear and easy to use pathways for customers seeking redress following suspected instances of bias.
- Encourage periodic publication of algorithmic impact statements and content moderation.
- Incentivize major cloud providers to solicit public feedback on the development and implementation of content moderation policies, practices, and technologies.
- Develop standards for oversight, accountability, and transparency of providers' polices and content moderation requests.
- Model domestic rules regarding service availability after principles such as Article 19 of the Universal Declaration of Human Rights.[16]

Ensuring a Beneficial and Safe Digital Environment for Groups with Special Requirements

- Promote standards and potentially offer incentives to ensure digital services are accessible and inclusive.[17]
- Prioritize enforcement of existing laws designed to protect vulnerable groups online.
- Differentiate and clearly define standards regarding how content harmful to children, seniors, and others is moderated, and by whom.

Privacy Protections

- Require greater transparency in cloud computing contracts between customers and providers, particularly around responsibility for data privacy, liability for breaches, obligations for reporting and remedial action.
- Require increased transparency by providers and their customers on the collection, usage, storage, deletion, and other actions of specific types of data on a sector-by-sector basis.
- Provide model language on how to clearly allocate responsibilities and rights of parties with respect to data privacy.
- Define the ways in which impacted individuals may seek compensation for damages.
- Work with foreign governments to establish international agreements and mechanisms to resolve conflicts of laws, in order to ensure the privacy of citizens' data as it moves across jurisdictions.
- Set guardrails for the degree of access governments may exercise in the event of government intervention.

Notes

[1] Requirements on disclosure timelines to government agencies vary both within and among nations, with some governments calling for 72-hour timelines and others for as low as 12-hours. These requirements may also vary depending on the function and sectors (such as, critical infrastructure and government services) being served. See: Michael Kans, "Congress Debates Cyber Incident Reporting Deadlines in the NDAA," Just Security, 26 October 2021, https://www.justsecurity.org/78745/congress-debates-cyber-incident-reporting-deadlines-in-the-ndaa/.

[2] While this occurs in the U.S. under the auspices of the Cybersecurity and Infrastructure Security Agency (CISA) and in other individual countries, not all governments maintain a centralized cybersecurity agency to perform this function. See: CISA, "Cybersecurity and Infrastructure Security Agency." Cybersecurity and Infrastructure Security Agency, n.d., https://www.cisa.gov/.

[3] See: Jay Greene Jay and Drew Harwell, "When the FBI seizes your messages from Big Tech, you may not know it for years," *The Washington Post*, 25 September 2021, https://www.washingtonpost.com/technology/2021/09/25/tech-subpoena-secrecy-fight/.

[4] See: U.S. Department of Justice, "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act," U.S. Department of Justice, April 2019, https://www.justice.gov/opa/press-release/file/1153446/download.

[5] Telecoms World, "Diverse Routing," Telecoms World, n.d., https://www.telecomsworld.com/diverse-routing.

[6] For example, in the case of the U.S., Congress enacted into law the Terrorism Risk Insurance Act, which created a backstop for insurance providers against large-scale, catastrophic losses arising from terrorism-related attacks, outside of the scope of war. Prior to this, insurance companies often used the "war exclusion" in their policies to avoid covering the claims that may arise from terrorist-related acts. See: Jon Bateman, War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions (Washington, DC: Carnegie Endowment for International Peace, October 2020), https://carnegieendowment.org/2020/10/05/war-terrorism-and-catastrophe-in-cyber-insurance-understanding-and-reforming-exclusions-pub-82819 and Aaron Klein and Scott R. Anderson, "A federal backstop for insuring against cyberattacks?" *The Brookings Institution,* September 27, 2019, https://www.brookings.edu/blog/techtank/2019/09/27/a-federal-backstop-for-insuring-against-cyberattacks/.

[7] These strategies can include arrangements for failover across regions, load balancers, application gateways, and more, and should as well include a complementary data backup strategy (for example, how frequent should the backup process be, how extensive, should they be simultaneous across all applications, and so on) and a strategy on how to address lost data. A disaster recovery plan should also account for the people, processes, and applications needed to restore functionality, and should be fully and regularly tested through disaster simulations.

[8] "SWIPO (Switching Cloud Providers and Porting Data), is a multi-stakeholder group facilitated by the European Commission, in order to develop voluntary Codes of Conduct for the proper application of the EU Free Flow of Non-Personal Data Regulation / Article 6 'Porting of Data.'" See: SWIPO, "Switching & Porting," SWIPO, n.d., https://swipo.eu/.

[9] Beyond Standards, "IEEE Addresses Standards for the Cloud," Beyond Standards (blog), IEEE Standards Association, April 18, 2011, https://beyondstandards.ieee.org/ieee-addresses-standards-for-the-cloud/.

[10] "ISO/IEC 19941:2017 specifies cloud computing interoperability and portability types, the relationship and interactions between these two cross-cutting aspects of cloud computing and common terminology and concepts used to discuss interoperability and portability, particularly relating to cloud services. See: ISO, "ISO/IEC 19941:2017: Information technology – cloud computing – interoperability and portability," ISO, December 2017, https://www.iso.org/standard/66639.html.

[11] This may include incidental uses of data and other reasonable uses, for example, such as those stipulated under "legitimate interests" in the General Data Protection Regulation (GDPR), "GDPR Legitimate Interests," GDPR, n.d., https://www.gdpreu.org/the-regulation/key-concepts/legitimate-interest/.

[12] "Brownfield" refers to sites that are often difficult to use for other purposes due to contamination, the presence of hazardous substances (for example, former gas stations and landfills). Development of these sites often requires significant investments in pre-development cleanup, revitalization, and monitoring to remain in compliance with local laws. Cloud providers are well-positioned, due to their size and affluence, to overcome these hurdles, reducing the development pressure on "greenfield" sites, undeveloped land that may be used for agricultural purposes. For additional information, please refer to: United States Environmental Protection Agency, "Overview of EPA's Brownfields Program," United States Environmental Protection Agency, n.d., https://www.epa.gov/brownfields/overview-epas-brownfields-program.

[13] For additional information, please refer to: Paul Gillin, "Data Center Operators Look to Cooling Strategies for Greater Efficiency," Data Center Frontier, January 15, 2021, https://datacenterfrontier.com/data-center-cooling-efficiency/; Matteo Mezzanotte, "Datacenter Cooling Methods: The Importance of Choosing the Right Cooling Method," Submer, October 13, 2015, https://submer.com/blog/datacenter-cooling-methods/ ; and Clarke Energy "Data Centre CHP/Cogneration," Clarke Energy, n.d., https://www.clarke-energy.com/applications/data-centre-chp-trigeneration/.

[14] For additional information, please refer to: David Mytton, "Data centre water consumption," *npj Clean Water* 4, no. 11 (2021), https://doi.org/10.1038/s41545-021-00101-w.

[15] For additional information, please refer to: American Coalition of Competitive Energy Suppliers, "What is Energy Choice?" American Coalition of Competitive Energy Suppliers, n.d., https://competitiveenergy.org/what-is-choice/.

[16] Catherine Howell and Darrell M. West, "The internet as a human right," *The Brookings Institution*, November 7, 2016, https://www.brookings.edu/blog/techtank/2016/11/07/the-internet-as-a-human-right/.

[17] Web Accessibility Initiative, "Web Content Accessibility Guidelines (WCAG) Overview," Web Accessibility Initiative, (July 2005) April 29, 2021, https://www.w3.org/WAI/standards-guidelines/wcag/.