Cloud Providers

Below are measures cloud providers 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 governments.)
- Work with governments 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 governments and enterprise customers.)
- Help customers understand their new or potentially modified responsibilities under future performance-based certifications.

Incident Handling Procedures

- Proactively identify and define in contracts and/or SLAs roles in incident response and crisis communication vis a vis different cloud incident scenarios.[1] (Shared with customers.)
- Collaborate in the development of standards to ensure confidentiality in sharing of sensitive incident information. (Shared with customers and insurers.)
- Provide timely notification to governments and impacted individuals in the event of a cloud incident. (Shared with customers.)
- Commit to disclosing information about their own security practices with appropriate government agencies to aid in incident response and recovery coordination internal security practices.
- Work with cloud providers, customers, insurers, credit rating agencies, and other key stakeholders to determine appropriate disclosure constituencies, documentation, and timelines.[2] (Shared with governments, customers, credit rating agencies, and insurers.)

- Perform system penetration and stress tests (potentially also including "bug bounty/White Hat hacker" programs) to assist in detection of vulnerabilities and simulation of incident response. (Shared with governments and enterprise customers.)
- Commit to sharing relevant incident information with other cloud providers to assist in the prevention or mitigation of potential spillover across cloud systems.[3]

Localization and Routing Requirements

- 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 functionality and resilience.
- Work with governments to jointly develop reference designs and technical artifacts[4] 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.[5]

Security and Privacy in Lawful Government Access

- Inform enterprise customers of government access requests in every circumstance permitted by law.[6]
- Publish, on a regular basis, transparency reports detailing aggregate statistics on government access requests (including requests received from foreign governments).[7] (Shared with enterprise customers.)
- Develop industry standards for challenging and, where appropriate, rejecting certain overbroad government access requests (for example, requesting unfettered access, encryption keys, ability to break encryption). (Shared with enterprise customers.)
- Dissuade government access requests that do not meet agreed-upon criteria (such as requesting unfettered access, encryption keys, ability to break encryption) and challenge these requests through legal actions and public relations.

Resilience

Data Retrievability and Back-up Arrangements

- Create multiple retrieval and backup strategies and mechanisms for each service offered and which develop contingency plans for widespread disruptions from diverse sources.[8]
- Provide customers with guidance materials in support of their development of disaster recovery and data restoration strategies.
- Regularly carry out drills to test disaster recovery plans. (Shared with enterprise customers.)
- Increase transparency of their global dependencies that may impact customers' capacity to retrieve and/or backup data.

- Consider adopting practices compliant with international and other key information security standards (such as SOC 2[9] and ISO27001[10]). (Shared with enterprise customers.)

Government Intervention in Extremis

- Work with governments to ensure customer data is protected in the event of intervention. (Shared with customers.)
- Implement technical fail-safes that ensure government intervention does not compromise the security of cloud services.
- Ensure enterprise customers are insured against potential abuse or data mismanagement in cases of intervention. (Shared with enterprise customers.)
- Participate in working groups between governments, providers, and enterprise customers to delineate clear "disaster level" thresholds for government takeover and eventual release. (Shared with governments and enterprise customers.)
- Increase cooperation with governments and enterprise customers by participating in joint preparedness exercises. (Shared with governments and enterprise customers.)

Insurance for Cloud Services

- Collaborate with insurers (and potentially governments) to offer comprehensive coverage for risks emanating from cloud failures.
- Provide insurers with visibility into their cloud technology and operations in order to inform the development of cloud insurance offerings
- Work with governments and insurers to assign concerned stakeholders responsibilities and liabilities in the event of a cloud incident (including a sophisticated attack by a nation-state). (Shared with governments, enterprise customers, and insurers.)
- Help identify the conditions under which government backstopping mechanisms would take effect. (Shared with governments, enterprise customers, and insurers.)

Portability and Interoperability

- Develop and promote (in coordination with other providers) voluntary industry norms on portability and interoperability (for example, advancing a "customer bill of rights" for workload portability that includes technical and operational [licensing] standards and principles, such as a "transparency declaration,"[11] to help customers understand available accommodations, which data can be imported and exported, as well as which data standards, formats, and file types are recommended, used, or available).
- Encourage agreement on common terminology and principles for portability and interoperability in consultation with governments and customers. Definitions for these terms have been formalized in standards, including SWIPO's Codes of Conduct,[12] IEEE's P2301/P2302,[13] ISO/IEC's 19941.[14] Develop appeals and complaint procedures[15] whereby customers may raise concerns associated with (in)action by providers.
- Adhere to existing standards on open-source code and applications.

Consumer & Enterprise Protection

Commercialization of Customer Data

- Voluntarily disclose more information about data-processing practices, including with respect to data sharing, the sale of data, and the categories of data collected and used. (This may be a competitive advantage as it can improve customer confidence in their cloud providers.)
- Provide transparency into the internal decision-making process regarding what consumer and enterprise-derived data will be used and for what purposes.

Effects of Cloud Market Concentration

- Participate in industry-led dialogues to develop and advance technical standards for portability and interoperability between major providers.[16]
- Adopt standards on fairness and transparency in contracting, pricing, and liability.

Prosperity & Sustainability

Environmental, Community, and Energy Market Impact

- Support cross-sector and -industry initiatives to reduce carbon emissions and harmful waste through the development of guidance materials and communication of best practices.
- Adopt use of more sustainable server cooling methods.[17]
- Commit to reduce and improve water usage in data centers.[18]
- Providers may need to also focus on carbon capture/removal strategies.
- Collaborate with utility companies to identify "brownfield" sites[19] for constructing dedicated utility-scale electricity generation projects. (Shared with governments and utility companies.)
- Support the construction of healthier and sustainable buildings (that is, buildings that utilize materials that are safe for humans and the environment, as well as easier to recycle) and possibly leverage existing resources.[20]
- Understand and mitigate the adverse impact of cloud infrastructure creation and operation on local communities. (Shared with governments.)
- Leverage existing carbon emission reduction initiatives (for example, the Climate Neutral Data Centre Pact[21] and the Transform to Net Zero Initiative[22]).
- Commit to regular public reporting on key sustainability indicators, including energy and water consumption and progress toward sustainability targets.
- Whenever possible, encourage supply chain vendors to adopt similar sustainability principles/best practices.
- Share information and lessons learned on building a more sustainable cloud computing business and physical infrastructure.[23]

- Create consultation requirements with local communities and evaluate existing adjudication mechanisms. (Shared with governments.)
- Encourage the transition to a more sustainable business through the use of internal carbon pricing.[24]
- Integrate carbon reduction requirements into procurement policies.[25]

Human & Civil Rights

Cloud Access Restrictions and Content Moderation

- Leverage best practices on transparency and accountability in restricting access and the development of content moderation tools.[26]
- Refrain from restricting access or moderating content in ways that do not meet agreed-upon public standards/procedures.
- Implement "notice-and-comment" procedure before adopting/updating content moderation policies, practices, and technologies.
- Provide transparency into content moderation policies, as well as requests[27] and how providers comply with them, in every circumstance permitted by law (that is, via permanent/temporary removal of content/suspension of services).
- Establish a review process whereby customers and end-users can challenge content removal by providers, the ability to do so is clear, and the procedure thereof is straightforward.
- Agree to adopt and promote the use of explainable algorithms[28] in their products as well as to subject their content moderation offerings to algorithmic audits by independent, third-party corporate auditors.[29] (Shared with independent, third-party corporate auditors.)
- Publish regular algorithmic impact statements.[30]
- Ensure developers of content moderation tools are trained on machine bias, diversity, inclusion, and equity issues.[31]

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

- Establish clear policies and robust technical mechanisms that prevent, discourage, and penalize customers from utilizing cloud services for exploitation of vulnerable groups.
- Ensure consumer-facing enterprise customers, such as social media platforms, offer built-in protections for children and other vulnerable groups on their platforms.[32] (Shared with enterprise customers.)
- Ensure that combatting exploitation minimally compromises user privacy or data encryption.
- Consider providing additional services at little or no cost to low-income individual users and certain emerging enterprises (for example, minority or woman-owned businesses).

Privacy Protections

- Set technical guardrails that discourage intrusions and continuously monitor/audit these protections for effectiveness.
- Create internal or engage external entities to investigate suspected breaches of user privacy.
- Provide robust technical mechanisms that allow customers to govern the collection and handling of their personal information.
- Clearly communicate to customers data collection, analysis, storage, and dissemination practices and policies; this can be in the form of easily accessible and digestible "principles."[33]
- Provide clear language on the allocation of responsibility between providers and customers for data privacy. (Shared with customers.)
- Ensure employees are well versed on corporate privacy principles and the pertinent laws and regulations.[34]

Notes

[1] Cloud providers and their customers should develop and integrate incident notification matrices in their SLAs and/or contracts, laying out each party's responsibilities in crisis communications. For instance, the Cloud Security Alliance sets out the following division of responsibilities for various cloud incident response scenarios: (1) For a security incident occurring in the platform or service layer for a PaaS or SaaS application, the response should be driven by the cloud provider; (2) if a security incident is occurring in the application layer for a PaaS application, the customer should be driving the response; and (3) in the case of a security incident occurring in the platform layer for an IaaS infrastructure cloud, the response should be driven jointly by the customer and the cloud provider to determine if it originated in the customer's environment or the cloud provider's environment. (See: CSA, "Cloud Incident Response (CIR) Framework," Cloud Security Alliance (CSA), 4 May 2021, https://cloudsecurityalliance.org/artifacts/cloud-incident-response-framework/.) Additionally, the retention of digital forensic evidence should be seen as a shared responsibility. (See: Ben Martini and Kim-Kwang Raymond Choo, "An integrated conceptual digital forensic framework for cloud computing," ScienceDirect, Digital Investigation, vol. 9, issue 2, November 2012, pages 71-80, https://www.sciencedirect.com/science/article/abs/pii/S174228761200059X.)

[2] 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/.

[3] This can be achieved through an Information Sharing Analysis Center (ISAC). For example, the Cloud Security Alliance runs the Cloud Cyber Incident Sharing Center (CloudCISC) which facilitates incident data sharing between participating cloud providers. (See: CSA, "CloudCISC," Cloud Security Alliance (CSA), n.d., https://cloudsecurityalliance.org/research/working-groups/cloudcisc/.) In order to be successful, members must participate equally and actively, which requires that they have the willingness and ability to discuss security incidents that have

affected their organizations. Participation in these programs by cloud service providers may not be uniform, with some members possibly contributing more actively than others.

[4] 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/.

[5] 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: MANRS, "MANRS for CDN and Cloud Providers," MANRS, March 1, 2021, https://www.manrs.org/cdn-cloud-providers/.

[6] See: Trusted Cloud Principles, "Principles," Trusted Cloud Principles, 2021, https://trustedcloudprinciples.com/principles/.

[7] Many cloud providers already produce information request reports on a voluntary basis, as part of their corporate social responsibility commitments. See: IBM, "IBM 1H 2021 Law Enforcement Requests Transparency Report," IBM, 2021, https://www.ibm.com/downloads/cas/DAGAKDJG and Microsoft, "Law Enforcement Requests Report," Microsoft, 2021, https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report.

[8] These strategies can include arrangements for failover across regions, load balancers, application gateways, and more, and should account for the people, processes, and applications needed to restore functionality. Moreover, they should be fully and regularly tested through disaster simulations. For example, Microsoft Azure's locally redundant storage is advertised as providing low-cost single region durability, geo-redundant storage for high durability across regions, and zonal redundant storage for intra-region high durability. See: Microsoft Azure, "Preview of Zonal redundant Storage for Backup data from Azure Backup," Microsoft Azure, September 22, 2020, https://azure.microsoft.com/en-us/updates/preview-of-zonal-redundant-storage-for-backup-data-from-azure-backup/.

[9] AICPA, "SOC 2 – SOC for Service Organizations: Trust Services Criteria," AICPA, n.d., https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.

[10] ISO, "ISO/IEC 27001: Information Security Management," ISO, n.d., https://www.iso.org/isoiec-27001-information-security.html.

[11] As advanced in the "Code of Conduct for Data Portability and Cloud Service Switching for Infrastructure as a Service (IaaS) Cloud services – CSP Transparency Statement," SWIPO, May 27, 2020, https://swipo.eu/wp-content/uploads/2020/10/SWIPO-IaaS-CSP-Transprency-Statement-version-2020-27-May-2020-v1.0.pdf.

[12] "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/.

[13] 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/.

[14] "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.

[15] As advanced in the "Code of Conduct for Data Portability and Cloud Service Switching for Infrastructure as a Service (IaaS) Cloud services – CSP Transparency Statement," SWIPO, May 27, 2020, https://swipo.eu/wp-content/uploads/2020/10/SWIPO-IaaS-CSP-Transprency-Statement-version-2020-27-May-2020-v1.0.pdf.

[16] For example: SWIPO IAAS Drafting Group, "Code of Conduct for Data Portability and Cloud Service Switching for Infrastructure as a Service (IaaS) Cloud services," SWIPO AISBL, May 27, 2020, https://swipo.eu/wp-content/uploads/2020/10/SWIPO-IaaS-Code-of-Conduct-version-2020-27-May-2020-v3.0.pdf and SWIPO AISBL, "Switching and Portability of data related to Software as a Service (SaaS)," SWIPO AISBL, July 8, 2020, https://swipo.eu/wp-content/uploads/2020/07/SWIPO-SaaS-Code-of-Conduct.pdf.

P&S

[17] See: 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/.

[18] David Mytton, "Data centre water consumption," npj Clean Water 4, no. 11 (2021), https://doi.org/10.1038/s41545-021-00101-w.

[19] "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. See: EPA, "Overview of EPA's Brownfields Program," United States Environmental Protection Agency, n.d., https://www.epa.gov/brownfields/overview-epas-brownfields-program.

[20] International Living Future Institute, "Materials Petal Intent," International Living Future Institute, n.d., https://living-future.org/lbc/materials-petal/#10-red-list; and U.S. Green Building Council, "What is LEED?" U.S. Green Building Council, LEED Architectural Standards, n.d., https://www.usgbc.org/help/what-leed.

[21] Climate Neutral Data Centre Pact, "Home page for Climate Neutral Data Centre Pact," Climate Neutral Data Centre Pact, n.d., https://www.climateneutraldatacentre.net/.

[22] Transform to Net Zero, "Home page for Transform to Net Zero," Transform to Net Zero, n.d., https://transformtonetzero.org/.

[23] Microsoft, "Sustainability tools and resources," Microsoft, n.d., https://www.microsoft.com/en-us/sustainability/tools-resources?activetab=pivot_1:primaryr5; Google, "Sustainability Homepage for Partners," Google Sustainability, n.d., https://sustainability.google/for-partners/; and Oracle, "CDP Climate Change Questionnaire 2020," Oracle Corporation, August 26, 2020, https://www.oracle.com/a/ocom/docs/corporate/cdp-climate-change-questionnaire-2020.pdf.

[24] Brad Smith, "We're increasing our carbon fee as we double down on sustainability," Microsoft (blog), April 15, 2019, https://blogs.microsoft.com/on-the-issues/2019/04/15/were-increasing-our-carbon-fee-as-we-double-down-on-sustainability/.

[25] Stephen Nellis, "Sales acts on climate, requiring suppliers to set carbon goals," Reuters, April 29, 2021, https://www.reuters.com/business/sustainable-business/salesforce-acts-climate-requiring-suppliers-set-carbon-goals-2021-04-29/.

[26] For example, the Santa Clara Principles lay out baseline standards on transparency, notice, and appeal, that companies engages in content moderation may subscribe to ("The Santa Clara Principles on Transparency and Accountability in Content Moderation," May 7, 2018, https://santaclaraprinciples.org/). Likewise, Article 23 of the EU's Digital Services Act (European Commission, "The Digital Services Act: ensuring a safe and accountable online environment," European Commission, December 15, 2020, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en), which calls for transparency on the use of automated moderation tools, including transparency on what the precise purpose of the tool is as well as indicators of the accuracy of its filters and safeguards against error.

[27] Though not a cloud service provider, Twitter offers a useful framework for delivering insight into content moderation requests levied by governments: Twitter, "Removal Requests," Twitter Transparency, n.d., https://transparency.twitter.com/en/reports/removal-requests.html#2020-jul-dec.

[28] The auditability of AI remains contentious due to the black-box nature of these systems as well as to the security and commercial concerns by providers over auditing the source code for their technologies. A potential avenue to consider may be the adoption of explainable artificial intelligence (XAI) algorithms, which follow the three principles of transparency, interpretability, and explainability. In doing so, auditors and end-users may be better able to examine the systems and determine how it is making decisions and whether the results of these decisions are as expected. For additional information please refer to: Amina Adadi and Mohammed Berrada, "Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI)," in *IEEE Access* 6, (Fall 2018): 52138—60, https://ieeexplore.ieee.org/document/8466590.

[29] While such audits are relatively uncommon given the sensitivity around providers' proprietary software, they are growing in popularity. Fore additional information please refer to: Alfred Ng, "Can Auditing Eliminate Bias from Algorithms," *The Markup*, February 23, 2021, https://themarkup.org/ask-the-markup/2021/02/23/can-auditing-eliminate-bias-from-algorithms and Rumman Chowdhury and Jutta Williams, "Introducing Twitter's first algorithmic bias bounty challenge," Twitter Engineering (blog), July 20, 2021, https://blog.twitter.com/engineering/en_us/topics/insights/2021/algorithmic-bias-bounty-challenge.

[30] See: Nicol Turner Lee, Paul Resnick, and Genie Barton, "Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms," *The Brookings Institution*, May 22, 2019, https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/.

[31] For example, see how developers can better understand and practice racial sensitivity: Jessie Daniels, Mutale Nkonde, Darakhshan Mir, *Advancing Racial Literacy in Tech* (New York City: Data & Society, 2019), https://datasociety.net/wp-content/uploads/2019/05/Racial_Literacy_Tech_Final_0522.pdf.

[32] Sarah Perez, "TikTok to add more privacy protections for teenaged users, limit push notifications," TechCrunch, August 12, 2021, https://techcrunch.com/2021/08/12/tiktok-to-add-more-privacy-protections-for-teenaged-users-limit-push-notifications/.

[33] For example, IBM, "Data and Security Privacy Principles for IBM Cloud Services," IBM, n.d., https://www-03.ibm.com/software/sla/sladb.nsf/pdf/7745WW2/$file/Z126-7745-WW-2_05-2017_en_US.pdf.

[34] This may already be reflected in existing training and regulatory compliance activities.