

NOVEMBER 2020

Cloud Governance Challenges: A Survey of Policy and Regulatory Issues

Ariel E. Levite and Gaurav Kalwani

Cloud Governance Challenges: A Survey of Policy and Regulatory Issues

Ariel E. Levite and Gaurav Kalwani

For your convenience, this document contains hyperlinked source notes indicated by [teal-colored text](#).

© 2020 Carnegie Endowment for International Peace. All rights reserved.

Carnegie does not take institutional positions on public policy issues; the views represented herein are those of the author(s) and do not necessarily reflect the views of Carnegie, its staff, or its trustees.

No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Carnegie Endowment for International Peace. Please direct inquiries to:

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

+ CONTENTS

Summary	1
Introduction	2
Security and Robustness	6
Resilience	11
Consumer Protection	14
Prosperity and Sustainability (Employment, Growth, Innovation, and Environmental Protection)	15
Human and Civil Rights	19
Intersections, Overlaps, Tensions, and Conflicts	20
Afterthought: Patterns of Regulatory Expression	23
Appendix: Recommended Reading	26
About the Authors	27
Acknowledgments	27
Notes	28

Summary

The rising importance of cloud services and cloud service providers (CSPs) in society has caught the attention of policymakers and regulators seeking to reap the benefits of this new technology while managing attendant risks. The regulatory landscape of cloud computing is highly complex, owing to factors such as its rapidly increasing centrality to many societal and economic functions and continuous innovations in involved technology. Understanding the many issues emerging from this context will be critical to responsibly unlocking the potential of cloud services for society.

To that end, this paper provides an overview of the many different policy issues related to the cloud that are either attracting or will soon attract attention from policymakers as well as advocates, consumers, and corporations. Principally, we highlight five baskets of policy and regulatory concerns pertaining to both CSPs and cloud services more broadly: security and robustness, resilience, consumer protection, prosperity and sustainability, and human and civil rights. In approaching these issues, we underscore the importance of taking into account the various perspectives through which different actors view cloud governance. In particular, we note four areas of focus and priority among these groups: those that examine the practices of individual CSPs, those that consider the features and implications of the cloud services market as a whole, those that focus on issues arising from dependence of individual and corporate consumers on cloud services, and finally those that look at the implications of government use of cloud services.

We emphasize the utility of such a multidimensional approach in capturing the scope, richness, and dynamism of the cloud phenomenon, and identifying the intersections and tensions between the various issues involved (especially given that these connections present potential challenges to the evolution of coherent policies and regulations). As the cloud affects ever larger swaths of human (and machine) interactions, we highlight the necessity of examining cloud policies and regulations from a global perspective to reflect the cloud's global reach. This state of affairs naturally implies that governance structures and solutions will inevitably differ between and within countries and regions due to divergent values, interests, and priorities that affect attitudes toward the cloud. We state the need for harmonization or at minimum some compatibility and reconciliation mechanisms between these many governance regimes. In the absence of such efforts, it may become largely impossible to reap the benefits of the cloud for global growth, innovation, prosperity, and stability. As such, this survey strives to overcome the common tendency to examine cloud-related issues from myopic, nationalistic, and siloed perspectives, and instead advance a global and holistic outlook that incorporates the various issues involved in cloud policy and regulation.

Introduction

Cloud service providers (CSPs) have become an increasingly important part of modern society. They enable a variety of critically important activities, empower numerous applications, and have increasingly come to store and process more and more sensitive data. Their centrality is now apparent not only in the digital economy but also in more traditional economic sectors, and indeed as an essential component of daily life. These developments spark the interest and concern of policymakers and regulators across the globe who aim in their respective jurisdictions to comprehend these trends, and to strike a balance between harnessing the benefits of the cloud revolution while moderating its adverse effects. Toward that end, this paper provides an overview of the diverse policy issues in cloud computing either already attracting or otherwise meriting serious attention and scrutiny from state, federal, and foreign policymakers and regulators in the next few years.

We principally highlight two different kinds of cloud governance issues:¹ (1) generic ones that have been present in other domains but are already or will in the foreseeable future become eminently applicable to the cloud as well; and (2) issues unique to cloud computing and CSPs that are becoming increasingly important as the industry expands, develops, and occupies a more central social, economic, and security role globally. It should be noted that this preliminary survey is intended for now solely as a tour d'horizon of the governance agenda. We do not aim to prognosticate, acknowledging that there is a great degree of uncertainty in each field we discuss. Furthermore, while we highlight the more contentious issues associated with cloud technology and its centrality, we do not presently suggest priorities (in importance or time frame) among the issues raised, nor do we propose recommendations for any specific set of cloud policy issues or regulations. Along the same lines, the survey is generic, not specific to any particular country or jurisdiction (although it does draw on examples for illustrative purposes).

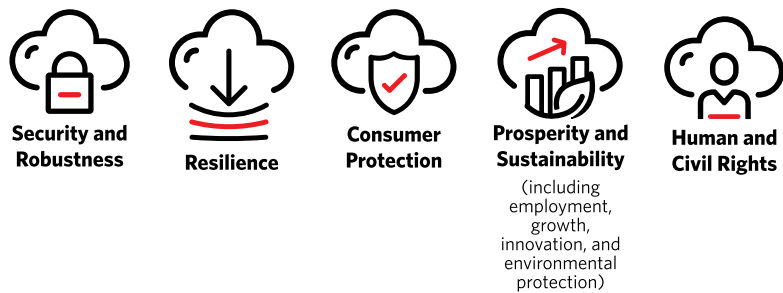
The issues discussed herein apply first and foremost to public cloud services that are accessible to any potential client of a CSP, as contrasted with private clouds dedicated to only one specific public or private organization. However, some of the governance issues inevitably also pertain (with some twists and turns) to the latter as well, especially for private clouds supporting government needs. Thus, we also recognize that increased government contracting with and dependence on cloud providers and their services will inform their general outlook toward cloud governance, and impact their policies and regulation in this domain far beyond the contractual arrangements they enter. Nevertheless, this delicate topic requires its own dedicated analysis, and so we do not examine it in detail in this paper.

For now, there is only a patchwork of policies and regulation pertaining to cloud services and CSPs; their maturity varies considerably across sectors and jurisdictions. In some localities and especially in certain domains, there already is existing legislation, for example concerning electronic communications or on handling sensitive personal information, that has been adapted to apply to cloud services, often imperfectly. In other cases, the challenges associated with cloud dependence have themselves only begun to be identified, and coherent policies or governance approaches have yet to emerge. A prime example concerns the data, processes, and especially applications hosted on the cloud or otherwise drawing on it. The platforms and programs that are based on or otherwise harness cloud services are thus far largely unregulated: determining who controls and regulates their use and on what basis, who decides what constitutes appropriate and inappropriate applications of user data, and how liability for cloud service setbacks (pertaining to availability, integrity, and confidentiality) ought to be adjudicated are just a few potential areas of importance here that have yet to be fully explored. This is just one of many emerging policy areas complicating governance efforts.

It is also important to note that much of the governance agenda concerning cloud services manifests not only vexing jurisdictional issues, but also differing perspectives between the various stakeholders and even outright conflicts of perspectives, values, and interests. The inherent tensions between different governance approaches necessitates careful consideration, prioritization, and balancing. We give some consideration to this added layer of complexity toward the end of this paper, and a follow-up publication will explore the issue in more detail.

Even without considering the tensions between them, the innumerable set of domestic, foreign, and international policymaking and regulatory authorities and standards setting bodies with pertinent say on cloud-related issues have prioritized certain areas over others. In some jurisdictions, privacy rights constitute the tantamount concern; for others, systemic risk to the economy or specific sectors thereof is of utmost importance. And for still others, access by certain governmental authorities (but not others) to the data stored on the cloud, and the capacity to both track and censor it, as well as the discretion of CSPs to do these things on their own, are the most critical issues. Thus, while competent authorities will inevitably differ on the priority as well as modalities they assign to addressing these concerns, they will likely all become significant issues in at least one regulatory environment. This fragmentation and differentiation combined with the global reach and centrality of the cloud inevitably means that the harmonization of policies and regulations is bound to prove an especially critical issue on a national and especially international level. Failure to manage and reconcile differences could result in serious degradation of the potential benefits of cloud services.

CLOUD GOVERNANCE ISSUES



For heuristic purposes, we have divided this paper into five baskets of issues:

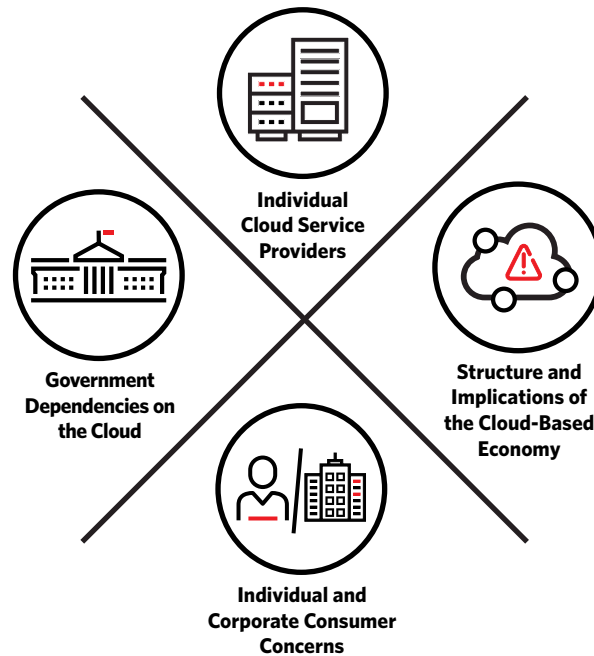
1. Security and robustness
2. Resilience
3. Consumer protection
4. Prosperity and sustainability
5. Human and civil rights

We have found it additionally useful to think of regulatory trends in terms of four different perspectives. These represent different lenses through which the various actors involved in cloud governance will assign priority and targets of policy, among other things:

1. Consumer dependencies on cloud services
2. CSPs as significant market players
3. The cloud services industry as a whole as a systemic force
4. Government dependencies on the cloud

PERSPECTIVES ON CLOUD GOVERNANCE

These symbols represent different lenses through which various parties approach cloud governance issues.



Each of these different lenses inevitably color the vision of those aiming to effectively govern cloud services; in approaching the myriad issues involved through their specific frame, they may overlook or underappreciate the broader implications of their enacted policies. A holistic approach toward cloud governance that aims to address and balance these interdependencies is thus acutely needed, much as it is far easier to recommend than to accomplish.

While it is analytically useful to employ these distinctions of frames and baskets to comprehend the cloud governance agenda, as will be done throughout this paper, it is also important to recognize that in practice these perspectives, issues, and policy solutions are interrelated and cross-cutting. For example, while concentration of market power in the cloud services industry can lead to considerable operational and cost efficiencies, these could come at the expense of lower levels of consumer protection, and also exacerbate certain security and resilience concerns.

Furthermore, some cloud governance issues are often misrepresented, or even deliberately masked by others for political or commercial reasons, making the already challenging discussion around cloud policy and regulation all the more difficult. One example is the heated debate around data sovereignty and localization standards. These policies are regularly presented as addressing security and privacy concerns, but often are in reality intended to promote economic and social interests, and especially to boost the growth of sophisticated data-driven domestic industry and services. A similar phenomenon can also be observed in the debate over policies on promoting 5G networks, which is hardly a coincidence, given that 5G core data routing networks themselves will be cloud-based.²

Below are the results of our preliminary survey of cloud governance horizons.

Security and Robustness

*This basket of issues concerns the ability of CSPs to plan for, protect against, and actively defend against both security threats to cloud services from malicious actions, as well as other perils arising from naturally occurring incidents, technical malfunctions, and human-induced accidents.*³

In essence, this area refers to the establishment of practices and systems to diminish the prospects that any or all types of malicious as well as nonmalicious events would compromise the availability, confidentiality, and integrity of equities clients assign to CSPs. The growing centrality of cloud dependence, and the escalating consequences of disruptions that come with it, are already motivating regulators to draw and expand on their established expectations of data security writ large and apply these to cloud services. In this sense, the emerging regulatory trends for CSPs are naturally inspired by, build on, or otherwise emulate these previous attempts to regulate the protection of data and operations, and create standards, transparency requirements, and safeguards thereof. These regulations may themselves also affect security and robustness, for example by raising compliance costs or requiring levels of access by government agencies that leave systems vulnerable to attack.

One key area for regulation is the delineation of the burden sharing, and codification of the “**shared responsibility**” for security and robustness between CSPs and their clients, and in some cases also the operators of supporting telecommunications networks.⁴ These models define the respective responsibilities of each party for securing data and underlying infrastructure, and are already emerging as a highly confused and contested space; there is significant concern that the asymmetric market power of CSPs over their customers could well produce unfavorable overall outcomes. As such, these models have the potential to be codified or altered by regulatory authorities in the same way as other types of contentious contracts and service user agreements of various social media and web applications in the past. Additionally, one cannot rule out some influence on this matter by court rulings

interpreting these contractual arrangements. In any event, the direction of such regulation could be informed inter alia by the aim of enhancing consumer protection, and attempt to prevent shifting of undue legal or technical burdens onto the consumer.

A subset of these issues that has already emerged as especially sensitive concerns the **migration process of data and services to the cloud**, be it at the beginning of service or when the parameters or scope of use changes or qualitatively expands. Regulators may expect CSPs at a minimum to be highly transparent on the allocation of responsibility and liability for any damages incurred in the migration process. Perhaps more ambitiously, they may also require that CSPs assume some responsibility to oversee their clients' migration of data and services, as well as development of cloud dependent applications, to ascertain that it is done in a manner that minimizes potential harm to customers' equities and also does not infringe on the overall security and robustness of the host cloud. The regulatory adjudication of issues in this space must factor in the objective difficulty of assessing (and periodically reassessing) the implications of evolving consumer dependence patterns on the cloud, which in turn are affected by frequently changing technological and commercial practices on both ends.

There is also likely to be increasingly charged policy discussion and regulatory action on the need for standards and adequate levels of transparency in **CSP security and risk management practices**, including both systemic controls and operational defensive measures. Such regulations may be similar to those enacted for other industries that perform vital economic functions and handle sensitive information. This includes not only cybersecurity and safety measures and practices, but also **physical protections and back-up arrangements** pertaining to both data centers and their supply chains as well as **underlying infrastructure**, especially telecommunications channels. Care must be taken in all cases to balance between transparency needs and the preservation of privileged information that is proprietary or critical to CSP security or business functionality.

All this brings to the fore the designation of cloud services as **critical infrastructure and CSPs as critical service providers**. At present, some of the biggest customers of CSPs (such as financial services, telecommunications, and power generation and distribution) are already formally designated in many jurisdictions (or at least practically treated) as critical infrastructure.⁵ Meanwhile, cloud services are increasingly becoming integral to the performance of these entities. This arrangement makes cloud services de facto part of critical infrastructure in and of themselves. But critically, CSPs also represent a separate but parallel huge risk aggregation potential, having become essential to the performance of a growing swath of other sectors that have not heretofore been massively dependent on centralized cloud functionalities, and hence vulnerable to their disruption. The sheer scale of these sectors' dependence on cloud services means that the potential economic loss (and social disruption) of even a brief lapse in service or a breach has grown exponentially, not to speak of graver scenarios

affecting prolonged outages or compromising confidentiality. As such, cloud services could evolve into platforms that consolidate rather than diversify **systemic risks**. Thus, regardless of whether they are formally designated as critical infrastructure, CSPs seem likely to be increasingly held to account by policymakers, legislators, regulators, the courts, and the media. Their security and robustness practices may be scrutinized at a level similar to designated critical infrastructures, though the modalities of such oversight may vary and focus on different types of concerns (for example, availability of service, susceptibility to malicious interference, and so on).

Definitional challenges also pervade the issue of **critical infrastructure designation**. As an example, U.S. lawmakers have recently requested that the Financial Stability Oversight Council (FSOC) investigate and regulate CSPs as examples of systemically important financial market utilities. These parties must meet higher risk management standards and are subject to increased scrutiny by the federal government.⁶ However, all the other entities in this category are financial clearinghouses or exchanges with clear connections to the global financial system, whereas CSPs are not themselves primarily financial actors. Designations also run into the issue of specificity as to what exactly should be deemed “critical”—the entire sector, a provider, a service, a particular function, a data center, or something else? Should regulation focus more on particular critical functions and industries using the cloud, or on the operation of data centers and infrastructure that enable these functions? The criteria regulators employ will determine the types and numbers of entities affected. It is also bound to raise profound jurisdictional issues, given that many of these entities and functions fall under the remit of diverse regulatory bodies.

While it is fashionable to discuss these issues primarily in terms of cybersecurity, it is as important to recognize that CSPs not only face malicious actor threats (hacktivists, criminals, terrorists, states and their proxies, and insiders) but also have to contend with accidents and technical malfunctions triggered by naturally occurring events, especially natural disasters (earthquakes, floods, storms, and so on). In fact, there have already been numerous cloud service and data center setbacks traceable to such causes.⁷ Sensitivity to these exogenous developments, not in the least when they affect auxiliary systems used by cloud services for power generation or communications, can be a serious source of disruptions and outages of cloud services. The various issues associated with **security and operational robustness** are therefore closely interlinked, and solutions for one cannot come at the expense of preparing for the other. Thus, they could potentially be fused together in pertinent regulation. Regulators will likely echo customers’ desires to see continuing progress toward ensuring robustness against all potential scenarios, and parallel developments that address concerns over not only service and data availability but confidentiality and integrity as well.

A related area of oncoming regulation is requirements surrounding responses to data breaches, including **data breach notifications**. In the United States, for example, individual states have taken independent action to impose notification requirements of their own, but there is considerable variance between state policies and no uniform regulatory standard that covers basic issues like protection obligations, reporting time, and required notification parties, as well as expected compensation or other remedial actions for those affected.⁸ Beyond implementing these requirements for data breaches, it is also conceivable that going forward there will emerge similar policies for other kinds of cloud service disruptions as well.

As the preceding discussion has indicated, for policy and regulatory purposes it is important to acknowledge that CSPs do not only provide data storage and processing capabilities. In fact, there are actually three major types of cloud services. The first type, Infrastructure as a Service (IaaS), refers to the basic functions just mentioned, namely data storage, processing, and networking. The second, Platform as a Service (PaaS), concerns the use of a cloud platform to build out and deploy different applications. Finally, Software as a Service (SaaS) covers any type of application or software hosted and accessed through the internet.⁹ Thus, cloud services encompass a wide variety of activities, and importantly can enable **complex applications and operations** such as those drawing on data mining or machine learning. These activities are just as important to many enterprises as regular data functions, and just as under threat from lapses in security and robustness. Furthermore, these activities also represent potential targets for malicious actors, who may, for example, attempt to steal or manipulate data inputs, or even gain access to cloud-hosted platforms for various purposes. State actors are also taking increased interest in such access, sometimes through legitimate means (generally when exercised domestically), or otherwise covertly as part of operations directed abroad. Governments may look to leverage cloud dependencies for homeland security, intelligence collection, information warfare, and even military operations.

Cloud-enabled end-user applications and products themselves could also be harnessed for malicious activities such as **disinformation and fraud** (as such, government agencies will additionally desire to have easy and discreet access to platforms for law enforcement and homeland security functions, as will be further discussed later). Thus, over time it is likely that not just data but also the applications and algorithms that harness it for various purposes are likely to become a growing policy and regulatory concern, not in the least for their security and integrity. Regulatory approval for entrusting vital operations in critical industries to such algorithms is bound to become an issue of growing sensitivity and importance. The fight over TikTok's "For You" recommendation algorithm, which China has placed export controls on amid the company's search for a U.S. buyer, emphasizes the critical importance of these algorithms and their potential to be regulated separately from the platforms on which they are hosted.¹⁰

The **infrastructure** that CSPs themselves depend on is another area of considerable concern. Obviously, some of the regulatory attention would be directed at CSPs that bundle together telecommunications and cloud services, building and/or operating private internet backbone networks, fiber optic landlines, and especially undersea cables to support their cloud offerings. Given the centrality of these communication links to the viability of cloud services, regulators have ample reason to require the application of standards and transparency for security in these infrastructures; related requirements could mandate contingency plans for any potential issues that may arise from their use or from disruptions that affect their functionality. This issue has been growing in importance given recurring indicators that some states have been developing capabilities to cut off vital communications links (especially underwater cables) to their adversaries during a crisis.¹¹

Another related issue is the security and integrity of the **supply chains** of vital equipment and services involved in data center and telecoms infrastructure construction and operation.¹² Regulators can be expected to seek guarantees that both hardware and software components, applications, and support services meet necessary security standards and are not vulnerable to compromise by malicious actors (this being one of the areas in which 5G policy concerns are similar to those of the cloud, given recent efforts by the United States to discourage other countries, especially allies, from using Huawei equipment to build out their networks).¹³ In general, governments may move to establish sovereignty and excise foreign involvement in all elements of internet infrastructure from hardware to software; one example is the U.S. government's recent "Clean Network" proposal aiming to remove all Chinese influences from the country's internet ecosystem (including specifically cloud services, represented as the "Clean Cloud").¹⁴

Concerns about infrastructure security are not only confined to the physical robustness of communication links. Commercial or operational considerations may motivate CSPs and other providers of cloud-based services to permanently route, or even occasionally reroute, cloud traffic through certain territories. While this may provide benefits in terms of efficiency, robustness, and resilience, such practices also make it at least conceivable that such traffic could then be intercepted, interrupted, and perhaps even manipulated. This concern recently accompanied revelations that the video conferencing company Zoom routed some of its calls through servers in China, which led the company to announce that more controls over data routing would be made available to its customers.¹⁵ Commercial or regulatory requirements for end-to-end encryption of the traffic to and from the cloud could somewhat diminish, but not eliminate, potential risks associated with such scenarios. Thus, cloud services are susceptible to government requirements that CSPs provide transparency on their **routing operations**, and potentially also commit not to route traffic through certain countries (or, on the flip side, requirements by certain governments that CSPs only route data through certain areas). In fact, governments may go much further and elect to ban or at least temporarily restrict domestically domiciled CSPs from performing any kind of services in or for certain countries, should they

perceive national security considerations to warrant such extreme measures. The same goes for potential banning or at least restricting (in terms of type of services offered or clients permitted) foreign CSPs' operation in the home country.

A final related area of potential regulation here pertains to **data localization**, which refers to requirements that data be stored and processed solely within a given jurisdiction. There are “hard” localization requirements, which stipulate that data not leave the jurisdiction, and “soft” requirements, which mandate that a copy of all the data be stored locally. “Soft” localization can also refer to regulations where export of data may be allowed under certain conditions (for example, if the destination meets a set of regulatory standards) or through specially designed transfer and reciprocity mechanisms.¹⁶ The development of such arrangements, such as the U.S.-EU Privacy Shield, will be of interest to regulators as a matter of security as well as business functionality (as the recent European Court of Justice ruling invalidating the Privacy Shield indicates, however, these arrangements will still be affected by differing policies and views on privacy, ethics, and other issues).¹⁷ As will be discussed later, localization requirements may be couched as addressing security concerns, but may also (even primarily) be driven by and have implications for industrial policy and economic development, as well as privacy and human rights considerations.

Resilience

This basket of issues pertains to measures taken to ameliorate the adverse consequences that may arise from service failures, disruptions, and other distortions to cloud-based services through contingency planning, backstopping, and insurance mechanisms.

Notwithstanding measures CSPs take to protect and defend against attacks, incidents, and accidents, it seems clear that such events are inevitable, as are the damages that may ensue as a result. As previously mentioned, some of these may be triggered by nondigital events associated with power failures or natural disasters as well as technical failures; the continuous expansion and transformation of cloud services will likely increase the frequency and variety of such events. Thus, resilience for CSPs means the ability to cope with and effectively recover from all events affecting cloud services that result in the loss of confidentiality, availability, or integrity of data and applications. This would also include cascading effects on clients and the economy/society writ large that could result not only in significant financial losses, but also potentially in serious property and casualty harm. This is one of the more unique issue categories to the cloud: the specific concentration of services in a handful of data centers, the critical importance of many of those services, and the nature of potential service interruptions or distortions are different than in most industries.

Contingencies in the event of breaches that lead to data exposure, loss, or corruption will likely attract considerable regulatory attention. Regulators may wish to set more stringent requirements (or more actively enforce existing ones) for **credible backups** to cloud services, and measures to minimize the consequences that flow from data and application loss and corruption caused by breaches, accidents, or attacks. However, given that regulator bandwidth and expertise are likely to be limited, and CSPs are likely to express opposition to invasive or overly ambitious steps, it's possible that regulatory measures will mainly be administrative in nature. In this case, priority may be placed on the development of institutionalized processes for **auditing services and reporting (and ultimately learning from)** adverse events.

More ambitious requirements to mitigate the risks that would materialize if a CSP undergoes an extended lapse or distortion in service could follow on at a later time, after governments develop a deeper understanding of involved issues and consult with CSPs on their operational and economic implications. Regulations in this vein could in particular include **interoperability and portability standards** (these will be discussed in more detail below as part of the consumer protection basket). Naturally, such standards would be more applicable to some types of services than others, and would likely have more utility for IaaS platforms than PaaS or SaaS, as an example. Thus, alternative methods of hedging risk might emerge through **hybrid cloud or multicloud strategies** and associated regulatory requirements and standards.¹⁸

Another important regulatory priority in the category of resilience is **insurance** as a risk channeling mechanism, to offset physical or financial damages resulting from cloud failures. Physical damage and bodily harm, should they occur as a result of cloud failure, could conceivably be covered by currently available insurance policies. The same goes for modest amounts to cover breach reporting and legal expenses associated with this type of event. However, it is presently unlikely that most other expenses and economic damages both caused by and affecting CSPs, especially events resulting in business interruption, let alone continuous business interruption, would be forthcoming. At present, little recourse is available to CSPs or the consumer to address such serious and likely scenarios. The nascent cloud insurance market does not currently offer extensive solutions to this predicament, in part because of serious concern for the systemic risk that accumulates as a result of the cloud's market concentration and the potential for cascading effects. System failures could potentially affect many different parties at once, trickling upward, downward, and sideways, and resulting in a mass of claims that could prove excessive for insurers and reinsurers to cover. Regulators' concerns over the solvency of (re)insurers that underwrite cloud services in these domains are bound to further slow down expansion of insurance for cloud service business interruptions, especially as they pertain to coverage of damages to third parties.¹⁹

Mechanisms to facilitate credible and responsible **expansion of the scope of coverage** available to CSPs, their suppliers, and consumers could thus emerge as a key regulatory goal. Regulators will ultimately want to ensure that a range of insurance products are both available and affordable to cover all parties, and as many as possible of their requirements and scenarios of concern (especially those associated with business interruption). They may also wish to ascertain that there is both **fairness and transparency** in contracting and in the provision of such products, and that the insurance products on offer will not present solvency issues for insurance providers; this will be a delicate balance to strike, as carriers are likely to balk at offering coverage for scenarios whose probability and consequences they have difficulty assessing and thus could exceed their appetite for risk.

One should note an additional cluster of related concerns. Some of the resiliency challenges could come from other scenarios affecting CSPs, such as financial woes, and in extreme cases outright **insolvency**. Society's level of dependence on just a few huge, market-dominating CSPs (and a handful of far smaller ones) makes such normal business scenarios especially scary, and finding arrangements to mitigate impacts (such as insurance, interoperability, portability, and continuance of service agreements) is thus bound to prove critical to smooth functioning of both the cloud market and the businesses that rely on it. Interestingly, the coronavirus crisis illustrates one extreme example of oncoming regulation in insuring against insolvency: the need for a category of insurance that covers events that stop businesses from functioning long-term without physical damage, such as pandemics or cyber attacks. This inevitably draws attention to the growing need to come forward with **government backstopping measures** for catastrophic events, especially as this type of event increases in frequency and grows in potential severity.

One final related concern pertains to the creation of **long-term digital preservation requirements and user-friendly retrieval mechanisms**. Because such activities can constitute a financial burden on service providers, impede operations, and potentially even slow innovation, they are unlikely to be undertaken voluntarily. However, a lack of such mechanisms would leave those dependent on cloud services with no long-term institutional memory. It is possible that this troubling situation could be rectified through public-private partnerships and individual and collective corporate initiatives, but ultimately there may arise a need for regulations to at a minimum encourage transparency on digital preservation obligations, if not outright requirements that CSPs retain data for some designated length of time.

Consumer Protection

This basket of issues centers around concerns over the relationship between CSPs and consumers due to the asymmetry of power between them, as well as the oligopolistic nature of the CSP market.

At present, the market for public, general-purpose cloud services is largely dominated by a few “hyperscale” providers such as Amazon, Microsoft, and Google (and Alibaba in China), each occupying a sizable market share and billions in industry profits.²⁰ In addition, the level of sophistication and complexity in the relationship between customers and their CSPs makes the former heavily dependent on the latter, due to the inherent difficulty and costliness of switching services. Put differently, the complex technology behind cloud services exacerbates risks of vendor lock-in. There are two main factors to consider here: the level of *interoperability* (how easy it is to make different cloud services work together as well as work with on-site consumer IT systems), and *portability* (how easy it is to switch data and applications from one cloud service to another, as well as from on-site systems to the cloud and back). Standards enabling both **interoperability and portability** of cloud services are likely to emerge as inter alia a means of avoiding vendor lock-in.

More broadly, the present characteristics of the CSP market predictably amplify some generic concerns. Asymmetry in power between providers and clients could lead to price gouging, lower quality of services, and fewer choices—even large and powerful enterprises have complained that they are at the mercy of CSPs when it comes to service negotiations. One additional unique facet of CSP market power distribution is that providers might be able to use and even sell data gleaned from customers for profit barring explicit contractual provisions that ban or restrict such practices, leaving customers with little choice or recourse if they wish to continue to reap the obvious benefits associated with dependence on cloud services. It is thus no surprise that there have been calls for standards requiring transparency in such practices, assessment of the value of such data, and perhaps even allocation of payments to those whose data is being sold.

An especially tricky related issue is the emergence, or even conscious introduction by CSPs (because of commercial or technical requirements, or perhaps in response to direct pressures of some governments and regulators) of meaningful **biases in the operation of cloud services** that favor some functions, customers, localities, sectors, or nationals over others. These biases may manifest themselves in terms of access, speed, security, availability, and more, and could present serious consumer concerns in an environment where there are only a few large CSPs that all operate this way. Both bias in the provision of cloud services as well as bias in the operations of cloud-hosted applications may

become salient issues for regulators looking to ensure fair and equitable access to such products. This has implications for consumer protection regulation and is also obviously of great concern in the economic basket of issues (see the next section).

Other key regulatory targets might include: fairness and transparency in contracting requirements, division of liability between CSPs and consumers, and scrutiny in market share/acquisition operations. In general, we should expect regulatory attention to focus over time on the protection of consumers against arbitrary decisions by CSPs to change the terms of their services, discontinue certain practices, engage in others, phase out support for certain products upon which consumers depend, and so on. Indeed, regulators in both the United States and Europe seem to increasingly favor addressing the power asymmetry between CSPs and consumers at the core, rather than dealing merely with some of its symptoms. In this regard, **reinvigoration of antitrust regimes** is emerging as a key approach to confront the anticompetitive practices of dominant players in the digital marketplace as a whole.²¹ Such efforts will be carried out not only in the name of consumer protection but also in the interest of promoting employment, innovation, growth, and welfare, and national competitive edge. These interests and their implications will be considered in the next section.

Prosperity and Sustainability (Employment, Growth, Innovation, and Environmental Protection)

This basket of issues focuses on the broader role and macro impact of the cloud in the domestic and international economic order, and policies aiming to leverage, channel, or redress effects on employment, growth, innovation, welfare, and the environment emanating from the evolution of the cloud services market and dependence on CSPs.

While the previous section discussed the relationship between CSPs and consumers, this section focuses on how CSPs affect their industry and the wider economy. As cloud services increasingly incorporate cutting edge technologies such as artificial intelligence, and ascend not just in size and diversity of services but also in their role in national economies and global business, various policymakers and regulators will focus more on their broader economic and social impact domestically and internationally. In particular, these actors will focus on the implications of cloud offerings for national growth, employment, innovation, competitiveness, and trade. It should be noted as well that these issues could just as easily be applied to subnational jurisdictions, such as states or provinces in a federal system and even cities, which have their own concerns as to industrial development. This

brings to the fore a preoccupation with issues such as equitable access to and geographical dissemination of cloud services, reliance on indigenous versus foreign cloud services, pace of adoption of cloud services generally and their more sophisticated applications in particular, and the overall impact of the cloud on the national as well as global economy.

As the dominance of hyperscale providers can affect the relationship between CSPs and consumers, so too can it affect the relationship of CSPs to the industry and wider economy. Most obviously, the dominance of a few large players over all other providers could result in establishment of **barriers to entry and market manipulation**. These concerns are often couched in terms of pricing, but it is important to highlight the nonmonetary consequences of market dominance as well. The **virtual integration (bundling) of digital services** by CSPs raises the concern that such practices could stifle innovation and erect barriers that disadvantage upstarts, all coming at the expense of customers and the economy writ large. These concerns are abetted by the perception of “**predatory**” practices by some of these big players accused of buying off or driving out of business innovative new companies that could challenge their dominance or undermine their business model. Of course, this behavior can also be directed from one hyperscale provider to another, particularly when one company has complete dominance in a particular area.

There is an additional and more unique challenge in the amount of useful data and other information that CSPs possess as a result of the services they provide, coupled with their remarkable **data mining and AI** prowess. Without proper precautions, it is possible they could use such capabilities in order to gain an unfair advantage in business, and expand and diversify their reach and power not only at the expense of most other enterprises, but also to the detriment of broader economic, social, and political interests. Policymakers as well as regulators will likely be wary of such outcomes, and they will be inclined to consider various measures that either check or limit the power of CSPs to perform such activities, or moderate the adverse systemic impact associated with their conduct.

Additionally, countries may be concerned over their **dependence on foreign CSPs** because of implications for protection against a bias in service availability, quality, and reliability, as well as handling of commercial and personally sensitive information, intellectual property, and certainly national security. Given these factors, countries inherently agonize between reaping benefits of economies of scale (that may mean entrusting cloud services to the leading global hyperscale providers) and promoting development of a domestic cloud services market either entirely on its own or in some form of collaboration with the foreign CSPs.

Naturally, the choices here are not equally available to every country and are partially influenced by the size and appeal of its market as well as its indigenous technical sophistication and infrastructure. In particular, the level of access citizens of a country have to **broadband infrastructure** in general

and the internet in particular will be an important factor in the development of any cloud market; initiatives to expand broadband access and equity will thus likely be a part of countries' cloud development strategies (5G policy will likely be relevant here as well). In general, **government support for the development, dissemination, and operation of cloud infrastructure** will likely emerge as an area of intervention aimed at boosting the indigenous economic benefits of cloud adoption.

An especially delicate and increasingly critical issue here arises from the ever more pronounced U.S. government inclination to leverage its market and financial power to impose sanctions, conditions, and other requirements not just on foreign companies wishing to operate in the United States but also on U.S. entities doing international business (a proclivity increasingly shared by China, partially as retaliation for U.S. measures). Such a trend raises the specter that the United States or others (China, India, and Europe are obvious candidates) could behave similarly toward CSPs domiciled (or majority owned by interests) outside their territory. The United States and China in particular could accomplish this using leverage arising from technological dependence on their components and/or manufacturing technology, or even the mere use of proprietary knowledge or currency. They may equally try to regulate or otherwise shape in some fashion international offerings of cloud service providers domiciled in their own country. These actions, especially by the U.S. but also by other governments, cannot be ruled out at some point in the business lifecycle, even if they initially elect to let such foreign contracting go forward. The prospects of such arbitrary and inconsistent behavior over time could compound restrictive effects and in turn strongly undermine the credibility of the cloud service offerings of U.S.- (and Chinese-) domiciled CSPs, encouraging foreign regulators to consider domestication requirements for some if not all cloud services as a hedge against U.S. (and Chinese) overreach.

Given these factors, there will likely be a mix of policy and regulatory actions in several countries (again, India, China, and Europe come to mind as the most immediate cases) aimed at both nurturing the **development of a domestic CSP market**, as well as discouraging, conditioning, or somehow **restricting (for example in terms of allowed functions) the local presence and offerings of foreign CSPs**. The availability of Chinese-domiciled CSPs that may be subject to even more heavy-handed (and far less transparent) governmental intervention in the foreign services they offer, could play into the hands of those policymakers and regulators that may wish to use ownership and country of domicile (and its legal system) as well as corporate governance structure as a criteria for determining their attitude toward CSPs.

Short of de facto outright bans on the operation of foreign CSPs (or at least of utilization of some of their services) in any national space, the above-mentioned concerns are also likely to manifest themselves in **data localization requirements**. As noted earlier, these policies are often couched in terms of national security or privacy concerns, even when the real or at least primary rationale is commer-

cial or political, and the actual goal of such policies is to make it more difficult for foreign CSPs to operate in-country, in order to open up the market for domestic actors. China, which already has some of the world's most stringent data localization requirements and is currently implementing more, enacted its localization laws for diverse economic and security reasons, but likely two significant factors were to bolster the Chinese CSP market, and to avoid what it saw as an unsafe level of dependence on the U.S. for cloud services.

On the flip side, policies and regulations that facilitate the development of **secure cross-border data transfer arrangements** will be a boon to corporations that operate in multiple countries, and these measures will thus have national and international economic impacts as well. Depending on the specific nature of localization laws enacted, the burden could fall heaviest on smaller companies that do not have the legal and compliance resources of the largest corporations, so data transfer arrangements could help to ensure a fairer market too.

Another issue regulators will have to consider is the **trade-off between standardization through regulation and innovation**. Some in private industry predictably caution that the bevy of existing or upcoming regulations, either through government actions or by trade and standards associations, have already constrained or will likely adversely impact the ability of CSPs to innovate, and thus could make for a less diverse and competitive services market. On the other side, concerns have been expressed that the meteoric rise and seemingly insatiable expansion of and acquisitions by CSPs could not only retard innovation but also lead to alarming power concentration in the hands of a few corporate giants. Balancing regulation to allow CSPs to continue to grow, expand their offerings to additional services, and prosper while still encouraging broader economic competition, innovation, and employment, will thus continue to be an ongoing challenge for regulators and policymakers in many countries.

Balancing regulation against industry concerns will also be relevant when it comes to **sustainability**. Although not the most common area of concern in regard to CSPs, data center operations use significant amounts of electricity (in part for cooling purposes) and carry a substantial carbon footprint.²² As such, providers may be subjected to **energy efficiency and emissions standards**. Some regulatory requirements could also stipulate a certain percentage of use of renewable/alternative energies to power data centers and set environmental standards in siting and constructing them. These regulations may also pertain to underlying backbone infrastructure on land and in undersea cables that could potentially raise environmental concerns. Siting requirements are a particularly salient issue, as the significant energy needs of data centers generally limit the number of locations in which they can be sited; regulators will have to balance energy needs and economic opportunities

with environmental implications at any given potential site. These regulations would likely be part of broader energy and environmental legislation or regulation, as well as voluntary industry adoption, and not necessarily as a CSP focused regulatory action.

Human and Civil Rights

This basket of issues focuses on concerns arising from the cloud's emergence as a huge depository of data and provider of increasingly essential services; individual citizens and groups within society may find their privacy and rights infringed upon, and their data and services disrupted, mined, manipulated, or otherwise leveraged by governmental authorities as well as commercial and criminal actors.

This is yet another issue that predates the emergence and widespread adoption of cloud services, yet is rising in prominence because of the increased use of cloud-enabled technologies. Public concern is rising over who can access user data and for what purposes, alongside increased scrutiny of functions such as facial recognition and location tracking. Cloud services, which enable or empower many of these applications and activities, are consequently in the crosshairs of privacy and human rights advocates (a trend that is all but bound to get stronger). Advocates will likely push at the very least for more **robust reporting and transparency requirements** surrounding data collection and storage arrangements, as well as guardrails pertaining to the applications they are put to (this could also include transparency on government requests for data, which some companies have already begun to release). More ambitiously, they might push for a higher level of **access, discretion, and control (including deletion rights) by individuals over their own data**, regardless of where it is located.

Data protection and the deeper values it embodies have already become a central issue in some of the largest cloud-relevant jurisdictions, including the United States, the European Union, India, and even China. Between them are sharp differences in focus and requirements, the priority they attach to these issues, and in their attitude toward differing viewpoints. These differences are partially rooted in and reflect political systems and cultures, but they also derive from particular economic, social, and political interests. Governments in some of these countries are most concerned with the ability of nefarious domestic and international actors (foreign governments and commercial entities alike) to **misuse cloud services**, while also being eager to facilitate, or at least far less concerned about, **access to the data by various government agencies**. Others focus on protection of **the privacy rights** of the individual and on enabling freedom of speech and association, especially in opposition to overzealous content moderation enacted in the name of security: Europe's General Data Protection Regulation, or GDPR, stands as the canonical example thus far, and its enactment has already had consequences for many cloud-related operations.²³

Still others worry that cloud-based data, services, and databases containing sensitive information constitute a treasure trove not only for their economic value, but also for their potential to empower authoritarian regimes to surveil, track, and micro-target with information and other actions their own citizens, and engage in manipulation of the populations in other societies, all while suppressing freedom of expression and association. States concerned about enabling such practices may elect to restrict corporations under their jurisdiction from exporting cloud services and technology to countries that abuse human rights.

Additionally, restrictions against **commercialization of information** for use in advertising and predictive analytics without consumer consent (or real choice) will also likely be a focus of privacy advocates; this may include **value assessment and remuneration for consumer data use**, as previously mentioned. **Data localization and sovereignty** are important as a facet of this set of regulatory issues as well—like with security, privacy concerns are another common justification for localization requirements, given that they prevent the movement of data to areas with potentially weaker privacy protections.






One more potential area of interest is in the evolving idea of **unhindered internet access as a basic right**; it is quite possible that advocates may eventually lobby regulators and other policymakers to consider extending this right to cloud access as well, given the increasingly important nature of cloud services in society (and particularly amid the coronavirus pandemic, when cloud and internet services have become more crucial than ever to the day-to-day functioning of society). On a separate note, concerns of equity may also extend to content hosted on the cloud and services offered by it as well, given increased interest in the need for political neutrality in platform moderation; there thus may be some form of “**equal time rule**” implemented for any platform hosting political content.

Intersections, Overlaps, Tensions, and Conflicts

The myriad issues presented here unsurprisingly capture the attention of a wide variety of stakeholders, including but not limited to: politicians, legislators, diverse government agencies (quite a few with some regulatory functions or with important input into them), private sector actors, policy advocates of various kinds, the media, and the public at large. At the same time, cloud technology and its applications are evolving at a breathtaking pace. This, in combination with the sheer number and complexity of issues, unsurprisingly produces a healthy measure of incoherence, inconsistencies (substantially and over time), and lacunas in the cloud policy and regulatory landscape. These problems are further exacerbated by the tensions and outright conflicts inherent in different regulatory interests and approaches, compounded by jurisdictional issues.

OVERVIEW OF CLOUD GOVERNANCE ISSUES

Below are five baskets of cloud governance goals, and means being considered for their attainment. These items highlight the scope and complexity of the cloud governance challenges involved.

 Security and Robustness	 Resilience	 Consumer Protection	 Prosperity and Sustainability	 Human and Civil Rights
<ul style="list-style-type: none"> ▶ Systemic controls and operational defenses to protect against unauthorized access, disruption of services, and manipulation of data, apps, and algorithms ▶ Law enforcement and homeland security access ▶ Allocation of responsibility and accountability for security between providers and consumers ▶ Applying safeguards to cloud supply chain and infrastructure ▶ Reliable processes for migration to the cloud (a continuous challenge) ▶ Localizing data and cloud operations to prevent compromise ▶ Cross-border data transfer arrangements ▶ Scrutiny and moderation (?) of uses and content to prevent misuse ▶ Designating the cloud as critical infrastructure (?) ▶ Continuity of service, government takeover in extreme duress 	<ul style="list-style-type: none"> ▶ Assured service continuity under duress (contingency planning, portability and interoperability of cloud service providers, data retrievability) ▶ Institutionalized process for reporting and learning from incidents ▶ Insurance coverage and carrier solvency for adverse events ▶ Governmental backstopping for catastrophes 	<ul style="list-style-type: none"> ▶ Preventing biases against consumers in services and applications ▶ Informing and rewarding (?) users for utilization of their data ▶ Protecting consumer privacy (data localization) ▶ Standardizing (?) contracting clauses to offset market concentration and power asymmetry between CSPs and consumers ▶ Informing and redressing compromise of confidentiality, integrity, and/or availability ▶ Preventing vendor lock-in (portability) ▶ Mandating interoperability among cloud services 	<p>(including employment, growth, innovation, and environmental protection)</p> <ul style="list-style-type: none"> ▶ Offsetting effects of excessive (?) CSP market concentration (anti-trust) ▶ Regulating CSP ownership, domicile, and location of infrastructure, and maintaining data sovereignty ▶ Cross-border data transfer and safeguarding arrangements ▶ Establishing widespread broadband access ▶ Government support for developing, disseminating, and operating cloud infrastructure ▶ Emissions and energy efficiency standards ▶ Environmental siting/ construction standards 	<ul style="list-style-type: none"> ▶ Protecting privacy, freedom of expression, and association: moderating/conditioning government access for tracking, surveillance, censorship, repression, and propaganda ▶ Upholding political neutrality in access and content moderation ▶ Restricting access to databases containing citizens' identity and vital information ▶ Establishing unhindered cloud access as basic right ▶ Restricting exports of cloud services to human rights abusers (?)

NOTES:

1. Many items listed here cut across different goals. In addition, items often exist in tension with one another; policies in the same category, as well as those oriented toward different goals, and even the goals themselves, can potentially conflict with each other, adding to the challenges of governance.
2. (?) = Items or phrases accompanied by this symbol represent issues most recently emerging in the policy and regulatory landscape, which even sophisticated actors may not have specific views on or even knowledge of.

Tensions in cloud governance exist on multiple levels; there are tensions between different concerns under one basket, between different concerns in different baskets, and between the overall baskets more broadly. Put another way, there can be tensions between different means of achieving the same policy goals, between means of achieving different policy goals, and between the goals themselves. Here we offer examples of each.

Within the same basket: The need for law enforcement, homeland security, military, and intelligence agencies to have unimpeded access to the cloud in order to protect against malicious threats, conduct surveillance, and engage in cyber operations (among other activities) may conflict with standards and requirements implemented for cloud security operations, especially those serving critical national functions.

Different concerns in different baskets: Data localization requirements implemented in the name of various economic and security interests can have negative effects on the ability of CSPs to secure their global operations as well as reap the overall economic impact of cloud services.

Between the baskets themselves: Measures taken to enhance security and robustness often come into conflict with human and civil rights concerns, especially when the former encroaches on data privacy and other individual freedoms.

Some of these conflicts are quite fundamental, anchored in values and core interests, and priorities stand in direct opposition to each other; the aforementioned debate on security vs human and civil rights is one example. Priorities here are difficult to reconcile, and governments to some degree will need to make choices that might not please advocates of either or both, because they involve striking painful compromises between two highly cherished objectives. Other tensions are more subtle, though no less important to consider in crafting policy or regulation; balancing between standardization and innovation to manage potential issues without compromising the dynamism of the cloud industry is a good example, as the relationship between the two is complex and not likely to be completely mutually exclusive. In all cases, choices will be subject to changing political tides, complicating the situation further for CSPs and other entities charged with compliance.

Additionally, tensions can emerge from multiple sources, and are not always ideological in nature. Often times, practical technological and operational realities prevent equal implementation of different types of standards. Consider the first example above: governments may require “backdoors” in cloud services that facilitate access for their agencies, while at the same time demanding that CSPs maintain a high level of security not only throughout their operations but also across their entire supply chain, which those same backdoors could make impossible or at least highly difficult to maintain. Reliance on third parties such as internet service providers can be another source of

tension, as factors outside of CSP control may dictate their responses to certain policy requirements, for example in data routing practices. Whatever the underlying reason, these tensions will be difficult to predict ahead of time, and indeed may not even be recognized given jurisdictional issues and siloing of interests. Given the importance of the governance dilemmas inherent in these intersections and tensions, they will be the subject of a more comprehensive discussion in a future paper.

Overall, given how tough some of the policy and regulatory challenges are likely to be, many issues associated with cloud governance will likely be addressed only partially, slowly, and suboptimally. The general lack of understanding and appreciation of the cloud and related issues by involved policy-making and regulatory authorities worsens this problem, highlighting the need for more robust education and engagement of relevant personnel (one of many goals of this document).

Afterthought: Patterns of Regulatory Expression

DRIVERS OF CLOUD GOVERNANCE	
Federal and provincial legislation and regulations	International treaties/agreements
Court rulings	Individual corporate self-regulation
Trade groups and other ESG (CSR) initiatives	Voluntary norms and standards set by domestic and international organizations
Informal demands by government authorities	Use of government purchasing and contracting power

It is beyond the scope of this preliminary paper to discuss in-depth the mechanisms by which these various regulatory concerns may be formally and informally addressed, and any conflicting requirements reconciled. Suffice to say here that because of the unique accumulation of issues and multifaceted attributes of cloud services, the tensions between them, their global relevance, and the considerable clout of some of the stakeholders, these are likely to take many and diverse forms. What form governance takes on any particular issue will depend on diverse political, economic, security, and cultural factors in each jurisdiction, and these approaches are bound to vary across time. Different methods may be applied toward the same goal, different agencies may be entrusted with the same task, and so on. Ideally, the pace and scope as well as the modalities of evolving domestic and global governance schemes would allow for sufficient flexibility to be adjusted over time in tandem with

technological developments as well as accumulating experience in dealing with cloud-related issues. In practical terms, this may make legislative efforts less desirable as a means of shaping such a rapidly changing field, given that laws are often challenging and time consuming to modify. In such cases it may be better to confine the role of legislation to high-level principles and guidelines whose implementation could be adjusted over time.

It thus also seems prudent to contemplate a broad range of other less formal governance structures that could be adopted and modified more easily. It is probable that in response to existing or anticipated regulatory pressures as well as public outcry, some norms and requirements in this space might emerge as preemptive or preventive industry actions to fend off or at least shape regulation in this domain. Regulators at various levels may then confine themselves to an oversight role, stepping in only when market forces fail to yield satisfactory results or require adjudication between sharply conflicting interests. Corporate actions could take the form of individual or collective self-regulation by CSPs, for example through trade associations or other ESG (environmental, social, and governance) initiatives, and/or voluntary endorsement of standards promulgated by the OECD (Organization for Economic Cooperation and Development), the ITU (International Telecommunication Union), and other international institutions and standards setting organizations.

Various courts will undoubtedly be another facet of the regulatory process as well, as they will inevitably weigh in over time on many of these issues, and may set important precedents as to rights and/or obligations of both CSPs and consumers, much as these may emerge piecemeal and produce inconsistent legal regimes among different jurisdictions. Finally, some of the efforts to influence CSP behavior may not come through explicit regulation, but rather through exercise of the government's market power. Cloud adoption strategies and trends in e-governance have made governments some of the largest and most important clients of CSPs. Governments will likely use their market clout and status as a large and powerful consumer as a source of leverage over industry to set standards of contracting fairness and other provisions that transcend the immediate cloud service contracts they enter. While formally these provisions will only apply to government contracts, they could over time cross over to the public clouds as well, or at least help set precedents that drive regulatory attention and inform industry standards. Yet over the longer run, government privatization of many services might actually weaken their leverage, given lock-in issues. How the balance between the two parties ultimately will play out remains to be seen.

The key issue to underscore here is the significant potential for the emergence of even more chaotic, disharmonized, and outright incompatible regulatory environments concerning CSPs both domestically and internationally. Consequently, ensuring interoperability or at least some sort of reconciliation mechanism within and between domestic regulatory structures of different countries will be necessary for CSPs to function effectively and legally in multiple jurisdictions. Early efforts to shape this environment could pay off handsomely, because rolling back or changing whatever regulation finally formally emerges is bound to prove difficult, costly, and at a minimum very time consuming.

Appendix: Recommended Reading

Allan A. Friedman and Darrell M. West, “[Privacy and Security in Cloud Computing](#),” Center for Technology Innovation at Brookings, October 2010.

Bruce Schneier, “[Censorship in the Age of Large Cloud Providers](#),” Lawfare, June 7, 2018.

Dunstan Allison-Hope, “[Taking Ethics to the Cloud](#),” BSR, April 10, 2012.

M. A. C. Dekker, “[Critical Cloud Computing](#),” European Network and Information Security Agency, December 2012.

Patricia Moloney Figliola, “[Cloud Computing: Background, Status of Adoption by Federal Agencies, and Congressional Action](#),” Congressional Research Service, March 25, 2020.

“[Global Data Governance Part One: Emerging Data Governance Practices](#),” *Foreign Policy*, May 13, 2020; and “[Global Data Governance Part Two: Evolving Government Data Collection Practices](#),” *Foreign Policy*, June 26, 2020.

Grace A. Lewis, “[The Role of Standards in Cloud-Computing Interoperability](#),” Carnegie Mellon University, October 2012.

“[Resiliency in the Cloud](#),” IBM, June 2015.

“[Cloud Down: Impacts on the US Economy](#),” Lloyd’s and AIR Worldwide, 2018.

Verena Weber, “[Cloud Computing: The Concept, Impacts and the Role of Government Policy](#),” OECD, August 19, 2014.

Tim Maurer and Garrett Hinck, “[Cloud Security: A Primer for Policymakers](#),” Carnegie Endowment for International Peace, August 31, 2020.

Trey Herr, “[Four Myths About the Cloud: The Geopolitics of Cloud Computing](#),” Atlantic Council, August 2020.

About the Authors

Ariel (Eli) Levite is a senior fellow in the Cyber Policy Initiative and the Nuclear Policy Program at the Carnegie Endowment for International Peace.

Gaurav Kalwani is a research assistant with the Nuclear Policy Program and Cyber Policy Initiative.

Acknowledgments

The authors wish to acknowledge and express gratitude for contributions and comments from our colleagues in Carnegie's Technology and International Affairs Program and Cyber Policy Initiative, including George Perkovich, Mike Nelson, Tim Maurer, and Monica Pellerano. We would also like to extend our thanks to Gare Smith, Chris Hart, and Christopher Fonzone for their thoughtful analysis and comments on various aspects of this paper. Sole responsibility for any errors or mistakes lies with the authors. Carnegie's Technology and International Affairs Program and Cyber Policy Initiative have received support from multiple funders which can be found [here](#).

Notes

- 1 We use the term “cloud governance” to refer to any policies, standards, or regulations promulgated by governments, industry groupings, individual corporations, and other relevant parties.
- 2 “5G Explained—Part Three: National Security,” *Foreign Policy*, published March 31, 2020, updated July 20, 2020, <https://foreignpolicy.com/2020/03/31/5g-cellular-huawei-china-networks-national-security-power-map/>.
- 3 For a more deeply focused overview of cloud security issues, see: Tim Maurer and Garrett Hinck, “Cloud Security: A Primer for Policymakers,” Carnegie Endowment for International Peace, August 31, 2020, https://carnegieendowment.org/files/Maurer_Hinck_Cloud_Security-V3.pdf.
- 4 See examples of such agreements from two of the largest CSPs: “Shared Responsibility Model,” Amazon Web Services, <https://aws.amazon.com/compliance/shared-responsibility-model/>; “Shared Responsibility in the Cloud,” Microsoft Azure, <https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>.
- 5 “Critical Infrastructure Sectors,” Cybersecurity and Infrastructure Security Agency, last updated March 24, 2020, <https://www.cisa.gov/critical-infrastructure-sectors>.
- 6 Pete Schroeder, “U.S. House Lawmakers Ask Regulators to Scrutinize Bank Cloud Providers,” Reuters, August 23, 2019, <https://www.reuters.com/article/us-usa-congress-cloud/u-s-house-lawmakers-ask-regulators-to-scrutinize-bank-cloud-providers-idUSKCN1VD0Y4>.
- 7 For examples, see: Declan McCullagh, “NYC data centers hit by Hurricane Sandy,” CNet, October 29, 2012, <https://www.cnet.com/news/nyc-data-centers-hit-by-hurricane-sandy/>; Ed Targett, “Azure Outage as Lightning Strike Forces Data Centre Offline,” Computer Business Review, September 5, 2018, <https://www.cbronline.com/news/azure-outage-microsoft>; “Missourti tornado destroys hospital data center,” Data Center Dynamics, June 9, 2011, <https://www.datacenterdynamics.com/en/news/missouri-tornado-destroys-hospital-data-center/>.
- 8 Drew Mitnick, “No more waiting: it’s time for a federal data breach law in the U.S.,” Access Now, April 10, 2018, <https://www.accessnow.org/no-more-waiting-its-time-for-a-federal-data-breach-law-in-the-u-s/>.
- 9 “IaaS, PaaS, and SaaS – IBM Cloud Service Models,” IBM, <https://www.ibm.com/cloud/learn/iaas-paas-saas>.
- 10 Russell Brandom, “Trump’s TikTok Deal Has Hit a Serious Roadblock,” Verge, September 2, 2020, <https://www.theverge.com/2020/9/2/21418496/tiktok-for-you-page-algorithm-deal-us-china-trump-microsoft>.
- 11 Garrett Hinck, “Evaluating the Russian Threat to Undersea Cables,” Lawfare, March 5, 2018, <https://www.lawfareblog.com/evaluating-russian-threat-undersea-cables>.
- 12 For a more in-depth overview of supply chain issues, see: Trey Herr, “Four Myths About the Cloud: The Geopolitics of Cloud Computing,” Atlantic Council, August 31, 2020, <https://www.atlanticcouncil.org/wp-content/uploads/2020/09/Four-Myths-About-the-Cloud.pdf>.
- 13 Julian E. Barnes and Adam Satariano, “U.S. Campaign to Ban Huawei Overseas Stumbles as Allies Resist,” *New York Times*, March 17, 2019, <https://www.nytimes.com/2019/03/17/us/politics/huawei-ban.html>.
- 14 Michael R. Pompeo, “Announcing the Expansion of the Clean Network to Safeguard America’s Assets,” U.S. Department of State, August 5, 2020, <https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/>.

- 15 Jay Peters, “Zoom Will Let Paying Customers Pick Which Data Center Their Calls Are Routed From,” *Verge*, April 13, 2020, <https://www.theverge.com/2020/4/13/21219835/zoom-data-center-call-routing-china-security-privacy-encryption>.
- 16 “Global Data Governance Part One: Emerging Data Governance Practices,” *Foreign Policy*, May 13, 2020, <https://foreignpolicy.com/2020/05/13/data-governance-privacy-internet-regulation-localization-global-technology-power-map/>.
- 17 “EU-US Privacy Shield for Data Struck Down By Court,” *BBC News*, July 16, 2020, <https://www.bbc.com/news/technology-53418898>.
- 18 Neal Matthews, “Hybrid Cloud vs. Multi-Cloud: What’s the Difference, and Why Does It Matter?,” *Cloud Technology Partners*, <https://www.cloudtp.com/doppler/hybrid-cloud-vs-multi-cloud-whats-difference-matter/>.
- 19 Ariel E. Levite, “The Cloud Challenge: A Multistakeholder Dialogue,” *Carnegie Endowment for International Peace*, October 27, 2020, <https://carnegieendowment.org/2020/10/27/cloud-challenge-multistakeholder-dialogue-pub-83050>.
- 20 Sooraj Shah, “Alibaba Versus Amazon, Microsoft and Google: Does the Chinese Cloud Challenger Have What It Takes?,” *ComputerWeekly*, February 11, 2020, <https://www.computerweekly.com/feature/Alibaba-versus-Amazon-Microsoft-and-Google-Does-the-Chinese-cloud-challenger-have-what-it-takes>.
- 21 “The House Antitrust Report on Big Tech,” hosted on *New York Times*, October 6, 2020, <https://www.nytimes.com/interactive/2020/10/06/technology/house-antitrust-report-big-tech.html>.
- 22 Charlotte Trueman, “Why data centers are the new frontier in the fight against climate change,” *Computer World*, August 9, 2019, <https://www.computerworld.com/article/3431148/why-data-centres-are-the-new-frontier-in-the-fight-against-climate-change.html>.
- 23 Alex Tolsma, “GDPR and the impact on cloud computing,” *Deloitte*, <https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-security-privacy-gdpr-update-the-impact-on-cloud-computing.html>.



1779 Massachusetts Avenue NW | Washington, DC 20036 | P: + 1 202 483 7600

CarnegieEndowment.org