nccr trade regulation
swiss national centre of competence in research

Working Paper No 2013/21 I AUGUST 2013

Cloud Innovation and the Law: Issues, Approaches, and Interplay

URS GASSER

FNSNF
Fonds national suisse
Schweizerischer Nationalfonds
Fondo nazionale svizzero
Swiss National Science Foundation

Die Nationalen Forschungsschwerpunkte (NFS) sind ein Förderinstrument des Schweizerischen Nationalfonds.
Les Pôles de recherche nationaux (PRN) sont un instrument d'encouragement du Fonds national suisse.
The National Centres of Competence in Research (NCCR) are a research instrument of the Swiss National Science Fondation.

Cloud Innovation and the Law: Issues, Approaches, and Interplay

Urs Gasser*

We live in a quicksilver technological environment where one innovation in information and communication technology (ICT) follows the other. From a user's perspective, the speed of innovation in the Internet age becomes particularly visible when looking at ever-changing hardware devices that enable instant access to information, knowledge, and entertainment, or when navigating the rapidly evolving social media space where new platforms and powerful services emerge periodically, like Instagram, Pinterest, and Quora.[1]

Many of today's trends and developments in the ICT space are powered by a less visible and arguably more evolutionary innovation at the lower layers of the ICT infrastructure: *cloud computing*. It describes a multi-faceted technological phenomenon in which important aspects of computing (such as information processing, communication, networking, data acquisition, storage, and analysis) move from local systems to more efficient, outsourced systems where third parties provide aggregated computational resources and services on an as-needed basis from remote locations. Cloud computing is arguably responsible, at least in part, for the speed at which new social platforms are being developed and brought to market.

This paper starts with a brief introduction to and framing of cloud computing as both a *technological innovation and innovation-enabling technology* – in short: cloud innovation. It then focuses on one particular aspect of the emerging cloud computing ecosystem by describing and discussing the *legal and regulatory responses* to cloud technology. It ends with general observations regarding the design of *interfaces* between cloud innovation as an example of an innovative and innovation-enabling technology and the legal and regulatory system.

The paper builds upon and aims to *synthesize* previous contributions by the author and his collaborators on cloud law and policy issues on the one hand and pattern recognition in ICT regulation on the other hand.[2] Against this backdrop, the paper seeks not only to distill and share

* Executive Director, Berkman Center for Internet & Society, Harvard University and Professor of Practice, Harvard Law School. The author wishes to thank David O'Brien for collaboration on this article, and Mira Burri for helpful feedback. Comments are welcome at ugasser@law.harvard.edu.

[1] Instagram, http://instagram.com; Pinterest, http://pinterest.com; Quora, http://quora.com.

[2] Urs Gasser and John Palfrey, "Fostering Innovation and Trade in the Global Information Society: The Different Facets and Roles of Interoperability" in Mira Burri and Thomas Cottier, eds., *Trade Governance in the Digital Age* (New York: Cambridge University Press, 2012), pp.123-153; Urs Gasser and David O'Brien, "Governments and Cloud Computing: Roles, Approaches, and Policy Considerations," (forthcoming 2013); Urs Gasser and Herbert Burkert, "Regulating Technological Innovation: An Information and a Business Law Perspective" in *Rechtliche*

insights about the interplay between cloud computing technology and the legal and regulatory system, but also contribute to a broader understanding of and emerging analytical framework for technology regulation in digitally networked environments.

1. Cloud Computing and Innovation

1.1 Overview

Cloud computing is a term that broadly describes an emerging group of related technologies and business models. For purposes of this paper, cloud computing is a broad label for technologies that enable the transition of computing resources – including information processing, collection, storage, and analysis – away from localized systems (i.e., on an end user's desktop or laptop computer) to shared, remote systems (i.e., on servers located at a data center away from the end user accessible through a network).[3]

Although cloud computing services can be modeled in a variety of ways, they are often described as fitting one of three models: *software as a service*, *platform as a service*, or *infrastructure as a service*.[4] The key distinctions between these models is in what the end user – who could be a consumer or an enterprise user – and the cloud service provider control and are responsible for maintaining in the solution stack.[5]

1.2 Service Models

The model where the end user is responsible for the least amount of management is the "software as a service" (SaaS) model, where a service provider remotely provisions software services in the application layer to end users through a network or over the Internet. SaaS represents the highest

---

Rahmenbedingungen des Wirtschaftsstandortes Schweiz: Festschrift 25 Jahre juristische Abschlüsse an der Universität St. Gallen (Zurich: Dike, 2007), pp. 503-523.

[3] Cloud computing has many definitions, nearly all of which are fraught with controversy and nuance from both technologists, industry experts, and scholars. *See, e.g.*, Geoffrey Fowler and Ben Worthen, "The Industry Is on a Cloud – Whatever That May Mean," *Wall Street Journal*, March 26, 2009, http://online.wsj.com/article/SB123802623665542725.html. The definition provided here is not intended to add to this debate, but rather to identify the components of this emerging trend as they have been described in popular media.

[4] *Cf.* Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing," US National Institute for Standards and Technology (NIST), Special Publication 800-145, September 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[5] The "solution stack" is a conceptual model for visualizing the distinguishable technological layers that compromise a system between two points (e.g., a service provider and an end user). In the case of cloud computing, at the highest levels of the stack are the software layers, which include individual applications (e.g., a word processor), middleware or software framework (e.g., Java), and operating system (e.g., Microsoft Windows or Apple OS X). Towards the lower portions of the stack are the physical infrastructure components, including the network and servers. These concepts will be explore in greater detail *infra* Section 2.2.

point in the stack, and incorporates the lower layers of services. The service provider maintains the software applications, the operating environment (the middleware and operating system layers), and the hardware infrastructure. An example of this is Google Docs, which enables users to use web-based productivity software through an Internet browser. "Platform as a service" (PaaS) and "infrastructure as a service" (IaaS) are also common models of cloud computing services. The services included in PaaS products typically fit into the stack layers below SaaS. In the PaaS model, the service provider provisions and manages a basic software computing environment (i.e., hardware architecture and an operating system or application framework) for running applications and programs created or licensed by the end user. Google, for instance, offers platform services through its App Engine, which provides a framework for developing and hosting web apps in common programming languages.[6] In the IaaS model, at the lowest layers of the stack, the service provider provisions only the hardware infrastructure, such as servers, processing power, storage, networks, and other physical resources, to the end user, who in turn uses the infrastructure to run arbitrary software (e.g., operating systems, applications and programs, etc). For example, Amazon offers basic infrastructure services through its "Elastic Cloud Compute" (EC2) services.

The basic abstraction model described above is more complex if third- and fourth-party intermediaries are included. At each layer in the stack the services can be provided by different entities and, effectively, chained together. For example, at the lowest stack layers – the hardware infrastructure – could be owned and operated by Amazon, while the layer the end user interacts with a higher layer (e.g., the application layer) that could be provided by a startup like Dropbox that rents the hardware infrastructure from Amazon. This characteristic has positive and negative effects, which will be discussed in greater detail in Section 1.4.

Beyond the type of services provided to the end user, cloud computing services can also be characterized by how the underlying infrastructure is operationally deployed: publicly, privately, or in a hybrid deployment.[7] In the public deployment model, cloud services are sold or offered to the public at large. End users in the public model are sharing the cloud service providers' resources, including servers and storage space, with each other. The cloud service provider typically owns and controls the infrastructure on their premises. In the private deployment model, the end users have exclusive access to the cloud services. This can be structured in two ways: the cloud service can be outsourced cloud-service provider who uses dedicated (non-shared) hardware infrastructure, or it can be managed by the end user (or by the end user's organization, in the case of enterprise users) on infrastructure by the user. In hybrid deployments, the cloud services are deployed through both public and private clouds. The deployment models can be differentiated by access exclusivity (whether the physical resources

[6] "Google Apps for Business," http://www.google.com/enterprise/apps/business/.
[7] *Cf.* Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing."

are shared with "outsiders") and degree of control as well as the location of physical infrastructure and maintenance responsibilities.

1.3 Cloud Innovation

Cloud computing as technological innovation

In terms of innovation theory, the concept of cloud computing is not necessarily revolutionary, rather it reflects the coalescence of a number of pre-existing technologies that progressed through a natural, evolutionary process to a point where cloud computing became economically and technically feasible.[8] However, the resulting ecosystem – combining different aspects of product, process, and structural innovation mainly at the intersection of technology and economics – produces a value greater than the sum of its parts. In turn, this evolutionary ecosystem is shifting the economics of ICTs and increasing the technological resources available to companies and individuals, enabling users to create innovations built on top of cloud computing services.

Public deployments of cloud computing are largely premised on the construction of large-scale data centers that contain upwards of 100,000 individual servers capable of parallel processing on a massive level. The computing resources of all these servers are effectively rented as "services" to a large number of simultaneous, remote end users, who, depending on the service model, utilize the raw hardware infrastructure (IaaS), software frameworks for other running other programs (PaaS), and web-based software applications (SaaS). Individually, the underlying technologies that comprise cloud computing – such as applied virtualization, parallel processing, the ability to deliver software services through a network, and so on – are by no means new. They have existed for many decades; but, they have recently evolved to a point of maturity where they can be centrally managed, coordinated, and provisioned to a large number of remote end users at scale. This controllable and well-coordinated ecosystem *is* new, and the synergies produced by the unity of the elements in the ecosystem are enabling innovative methods for delivering IT services, new uses of technology, and new business models.

The cloud computing ecosystem is capable of delivering several overlapping benefits that together differentiate its service models from other models of consumption: elastic, scalable computer resources; consumption-based pricing; and, minimization of operational expenses and elimination of upfront investments.[9] The computing resources are capable of scaling rapidly, and can be configured to respond to sharp increases in demand. The resources can also process

---

[8] *See* Erica Naone, "Conjuring Clouds: How engineers are making on-demand computing a reality," *MIT Review*, June 23, 2009, http://www.technologyreview.com/article/413981/conjuring-clouds/.

[9] *Cf.* Michael Armbrust, et al., "Above the Clouds: A Berkeley View of Cloud Computing," UC Berkeley Reliable Adaptive Distributed Systems Laboratory (February 10, 2009), http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf.

computationally-intensive tasks in parallel – as articulated by one group of scholars, a task that would take one computer a thousand hours to complete can be completed in the cloud by a thousand computers in one hour for the same price.[10] The pricing models of cloud services are typically pegged to actual use. This means end users only pay for what they use, regardless of how long or short and how big or small. This principle applies not only to computational tasks but also to other abstract layers of the cloud, including applications, software environments, and storage; computational resources can be bought and sold much like a commodity or a utility service. Finally, cloud computing service delivery models eliminate the need for upfront investments in infrastructure or long-term commitments to use services, and can drastically reduce operational expenses associated with maintaining traditional IT assets over time. This allows end users to reallocate risks and lowers the barriers for participation for new market entrants.

Cloud computing as innovation-enabling technology

While cloud computing itself is a technological innovation, it is also an enabler of *downstream innovation* – in other words, an innovation-enabling technology. End users are using cloud computing services to develop and power novel creations in nearly every industry.[11] Cloud computing can provide computational power to places where previously it did not exist. To give a brief sense of how the landscape is being shaped, consider the following examples. The computational resources in cloud computing can be used to extend the usability of software applications on lower-power devices, such as tablets, mobile phone, and netbooks. Mobile devices represent one of the fastest growing sectors in consumer and enterprise technology. Due to the constraints of the lightweight designs and small form factors of these devices, which necessitate small batteries and efficient processors, they must use power conservatively and as a consequence are not capable of performing computationally-intensive tasks. However, by accessing the scalable power available through cloud computing services, these devices can provide to users many of the functions that their more powerful cousins are capable of performing, and perhaps more. This could have enormously positive implications for developing regions of the world where the primary means of accessing the Internet is through mobile devices.[12]

Cloud computing is also enabling *entrepreneurs* to compete in industries and markets where large capital investments in infrastructure are necessary to get off the ground but outweigh the risks presented by a new venture or where traditional resources could not be deployed in a timely

[10] *Id*.
[11] *See* "Down on the Server Farm," *The Economist*, May 22, 2008, http://www.economist.com/node/11413148.
[12] Quentin Hardy, "Cloud Computing for the Poorest Countries," *New York Times*, August 29, 2012, http://bits.blogs.nytimes.com/2012/08/29/cloud-computing-for-the-poorest-countries/; *see also* David J. Hill, "Stethocloud – the $20 Stethoscope Attachment for Smartphones To Diagnose Pneumonia," *Singularity Hub*, August 10, 2012, http://singularityhub.com/2012/08/10/stethocloud-the-20-stethoscope-attachment-for-smartphones-to-diagnose-pneumonia/.

fashion.[13] Using cloud-based services, new ventures can quickly scale resources to accommodate a large influx of users in a short period of time, becoming competitive faster. Previously, it may have taken months to acquire and scale the necessary infrastructure and expertise in-house. Now startups can mimic the infrastructure capabilities that were once available only to companies with vast financial resources on hand in a matter of hours. But cloud computing also has applications that are attractive for other reasons beyond infrastructure savings. It enables companies of all sizes (as well as consumers) streamline their use of commodity software applications – such as, email, productivity suites, internal calendars, and so on. By using SaaS in lieu of licensed software installed on workstations and laptops locally, a company or individual can avoid the need for a costly IT staff, licensing fees, and maintenance, potentially increasing economic rents. These types of applications offer flexible and collaborative work environments with cost savings.

1.4 Drivers, Inhibitors, and Implications

Drivers

As noted in the previous section, the public cloud computing model is tied to large-scale data centers in conjunction with other enabling technologies and competitive advantages, such as virtualization, multi-tenancy, network infrastructure, and operational expertise. A *mixture of factors* are driving the supply and demand sides of cloud computing services.

The operators of large-scale data centers are driven by attractive margins, the ability to take advantage of economies of scale, and operational expertise. These are passed down to end users in the form of services priced to compete with traditional models of IT asset management. Purchasing servers and other infrastructure architecture in bulk yields at lower prices. Data centers are often constructed in remote areas of the country, where labor, energy, taxes, and real estate costs are far lower than elsewhere. Despite the sheer size, most large data centers can be managed by a relatively small number of on-site employees, bringing in additional cost savings. Many cloud computing service providers, particularly those who own and operate their own infrastructure, became providers to leverage their existing infrastructure. Amazon is a prominent example of this phenomenon. It developed an innovative method for internally scaling its own infrastructure, which experiences notorious peaks in demand around the holiday season, and eventually determined that the same techniques and infrastructure could be sold to the public.[14] Consumer-facing companies, like Facebook, have also turned into cloud computing platforms. Facebook provides a platform for software developers to write and distribute innovative apps to

[13] *See, e.g.*, Quentin Hardy, "Active in Cloud, Amazon Reshapes Computing," *New York Times*, August 27, 2012, http://www.nytimes.com/2012/08/28/technology/active-in-cloud-amazon-reshapes-computing.html.
[14] *See* Jack Clark, "How Amazon exposed its guts: The History of AWS' EC2," *ZDNet*, June 7, 2012, http://www.zdnet.com/how-amazon-exposed-its-guts-the-history-of-awss-ec2-3040155310/; Benjamin Black, "EC2 Origins," January 25, 2009, http://blog.b3k.us/2009/01/25/ec2-origins.html.

its more than one billion users. In this context, becoming a cloud service provider can be synonymous with creating an entire market.[15]

Not every cloud computing "service provider" owns and operates a data center. As noted earlier, the cloud computing model has introduced a new market for intermediary service providers, which serve as providers that fit somewhere between the infrastructure and the end user layers in the stack. This phenomenon illustrates the multifaceted value that cloud computing can provide as both an innovative technology and an enabler downstream innovation. One example of this is Dropbox, a company that offers free and paid-for cloud-based storage, which users can access and synchronize across a multitude of devices.[16] Dropbox does not own any infrastructure; rather it deploys a layer of software and graphical user interface atop Amazon's "Simple Storage Service" (S3), making the company more like a SaaS provider and an infrastructure reseller of sorts.[17]

The move towards cloud computing is also driven by fundamental shifts in the consumption patterns of consumers and enterprise users, who seek streamlined available-from-anywhere services on a variety of devices, spanning their home computer, mobile phone, and tablets. Users are also generating more data than ever before; pictures, videos, SMS messages, emails, and posts to social networks represent only the tip of a very large iceberg. To harness these data sources and provide value to the consumer, companies need powerful infrastructure. Innovative services, like Instagram, Dropbox, and Netflix, all of which rely heavily on infrastructure and storage, probably could not have become so popular in such a short period of time without the support of cloud computing services.[18] The implication is that any company or individual with an innovative idea, but limited financial resources, can deploy their idea at scale with relatively little upfront investment and expertise. In its other applications, cloud computing offers cost savings, an attractive risk profile, and an agile platform for creating bringing innovation to market.

---

[15] Michael Fitzgerald, "Cloud Computing: So You Don't Have to Stand Still," *New York Times*, May 25, 2008, http://www.nytimes.com/2008/05/25/technology/25proto.html.

[16] Dropbox, http://dropbox.com/.

[17] Dropbox, "Where does Dropbox store everyone's data?," https://www.dropbox.com/help/7/en. Amazon Simple Storage Service, http://aws.amazon.com/s3/. It is worth noting that these in-between service providers create interesting hybrid service providers that may be differentiated from the three deployment models noted in the previous section. For instance, the terms "storage as a service," "network as a service," and others are frequently used within the industry.

[18] *See, e.g.*, Quentin Hardy, "Active in Cloud, Amazon Reshapes Computing," *New York Times*, August 27, 2012, http://www.nytimes.com/2012/08/28/technology/active-in-cloud-amazon-reshapes-computing.html; Quentin Hardy, "Box and Dropbox Come of Age in Cloud Computing," *New York Times*, July 31, 2012, http://bits.blogs.nytimes.com/2012/07/31/box-and-dropbox-coming-of-age-in-cloud-computing/.

Inhibitors and Risks

While cloud computing promises much, it faces a number of *obstacles and challenges* that may impede or foreclose its adoption, spanning technological complications, cultural resistance, and uncertain applications of law and policy now or in the future. Many of the underlying architectural characteristics that make the cloud computing model unique – such as its centrality, multi-tenancy, and outsourced management – also give rise to overlapping concerns over its practicality. This section highlights a few of these potential inhibitors and risks; others, including the interaction between the legal system and cloud computing, will be discussed in greater detail in the subsequent sections of this paper.

From the *technical perspective*, potential inhibitors to cloud innovation and adoption include reliability, interoperability, performance issues, privacy, and security. In a cloud computing environment, the software and data is centralized; it resides on the cloud-service providers' systems. This introduces a potentially critical point of failure and a central vector of attack. If a single cloud service provider were to have an outage or experience a sweeping breach of security, it could have devastating effects on not just one business but thousands that rely on the availability of its services.[19] Several incidents have already publicly highlighted how cloud services are vulnerable to such failures, including one which reportedly impacted more than 700,000 websites in 2013.[20] A number of commentators have also pointed out how the centralized nature of cloud computing is an attractive target for security breaches.[21]

Technical incompatibility between cloud systems also presents an interoperability challenge for the innovative potential of the cloud.[22] For any number of reasons – e.g., costs, functionality, or

[19] K.F.C., "The Hidden Risk of a Meltdown in the Cloud," *MIT Technology Review*, March 13, 2012, http://www.technologyreview.com/blog/arxiv/27642/.

[20] Romain Dillet, "CloudFlare was Down Due To Edge Routers Crashing, Taking Down 785,000 Websites, Including 4chan, Wikileaks, Metallica.com," *TechCrunch*, March 3, 2013, http://techcrunch.com/2013/03/03/cloudflare-is-down-due-to-dns-outage-taking-down-785000-websites-including-4chan-wikileaks-metallica-com/; *see also* Tom Warren, "Microsoft blames overheating datacenter for 16-hour Outlook outage," *The Verge*, March 13, 2013, http://www.theverge.com/2013/3/14/4102720/outlook-outage-overheating-datacenter; Bob Darrow, "Will Amazon outage ding cloud confidence?," *GigaOm*, June 15, 2012, http://gigaom.com/cloud/will-amazon-outage-ding-cloud-confidence/; Claire Miller, "Amazon Cloud Failure Takes Down Web Sites," *New York Times*, April 21, 2011, http://bits.blogs.nytimes.com/2011/04/21/amazon-cloud-failure-takes-down-web-sites/.

[21] *See, e.g.*, Paul Lilly, "Is 'cloud security' an oxymoron?," *ExtremeTech*, August 8, 2012, http://www.extremetech.com/computing/134115-is-cloud-security-an-oxymoron; Jon Brodkin, "Dropbox confirms it got hacked, will offer two-factor authentication," *Ars Technica*, July 31, 2012, http://arstechnica.com/security/2012/07/dropbox-confirms-it-got-hacked-will-offer-two-factor-authentication/; Mat Honan, "How Apple and Amazon Security Flaws Led to my Epic Hacking," *Wired*, August 6, 2012, http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/all/. .

[22] *See, e.g.*, Barb Darrow, "Fear of lock-in dampens cloud adoption," *GigaOm* February 26, 2013, http://gigaom.com/2013/02/26/fear-of-lock-in-dampens-cloud-adoption/; Quentin Hardy, "Open vs. Closed: The Cloud Wars," *New York Times*, October 9, 2012, http://bits.blogs.nytimes.com/2012/10/09/open-vs-closed-the-cloud-wars/. For a general overview, *see* Urs Gasser, John Palfrey, and Matthew Becker, "Mapping Cloud

needs – a user may wish to terminate relationships with existing cloud computing vendors in order to move to a competitor. While the industry is developing standards, few currently exist to make data portable between service providers.[23] Other factors, like restrictive contractual terms or closed data formats, can make this technically difficult or prohibitively expensive. To some extent, cloud computing service providers have an interest in making their services as "sticky" as possible to minimize loss of customers to competitors. Fear of being locked into a particular provider and the lack of interoperability-enabling standards have reportedly held back many companies from migrating to cloud computing services.[24]

Because cloud computing relies heavily on a number of technologies, some in control of the service provider and others controlled by intermediaries between the provider and the service users, there are a number of factors that could sour performance.[25] The problem is twofold: the cloud may not provide benefits and adequate performance for the user, and it may not be able to perform more economically than a traditional IT approach.[26] Commentators have noted data transfer bottlenecks, scaling computational loads and storage, bug hunting, and patching are known obstacles that can unpredictably inhibit performance and dissuade potential adopters from using the cloud.[27] Another dimension is problems that arise between different providers in the cloud stack – for example, technical glitches or disputes between the IaaS provider and the SaaS, which may be distinct entities – also pose risks to end users.

The multi-tenant nature of public cloud computing services poses at least *two emerging risks*: security and privacy breaches from neighboring tenants and liability linking. Although many cloud-service providers go to great lengths to secure the partitions (the "virtual walls" between tenants), experts agree that multi-tenancy poses risks.[28] The risk is not only that a tenant might be able to breach other tenants' space, but also that an intruder of one tenant can gain access to

---

Interoperability in the Globalized Economy: Theory and Observation from Practice," *Berkman center Research Publication No. 2012-19* (June 1, 2012), http://ssrn.com/abstract=2192641.

[23] *See* Sixto Ortiz, Jr., "The Problem with Cloud Computing Standardization," *InfoQ*, September 2, 2011, http://www.infoq.com/articles/problem-with-cloud-computing-standardization.

[24] *See supra* note 22.

[25] *Ars Technica* recently featured an in-depth article on the performance issues with video buffering and playback at YouTube, one of Google's most public-facing cloud computing services, that illustrates a few aspects of the intermediary risks in the cloud, including the complex business and technical arrangements related to the Internet's backbone and how they impact performance. Jon Brodkin, "Why YouTube buffers: the secret deals that make – and break – online video," *Ars Technica*, July 28, 2013, http://arstechnica.com/information-technology/2013/07/why-youtube-buffers-the-secret-deals-that-make-and-break-online-video/. For an academic overview of these issues, *see* Susan Crawford, *Captive Audience: The Telecom Industry and Monopoly Power in the New Gilded Age* (New Haven: Yale University Press, 2013).

[26] Steve Lohr, "When Cloud Computing Doesn't Make Sense," *New York Times*, April 15, 2009, http://bits.blogs.nytimes.com/2009/04/15/when-cloud-computing-doesnt-make-sense/.

[27] *See* Michael Armbrust, et al., "Above the Clouds: A Berkeley View of Cloud Computing," UC Berkeley Reliable Adaptive Distributed Systems Laboratory (February 10, 2009), http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf.

[28] Press Release, "Gartner Says 60 Percent of Virtualized Servers Will Be Less Secure Than The Physical Servers They Replace Through 2012," *Gartner*, March 15, 2010, http://www.gartner.com/newsroom/id/1322414.

the digital assets of another. In this type of environment, ensuring compliance with regulations related to the handling of sensitive information, such as health and financial data, is complicated, which means that a public cloud might not be practical for certain types of industries, like healthcare or financial services. Sharing virtual space with others also has the effect of transferring liability and reputation. In one extreme example, servers from a website that provided digital locker storage services were seized in 2012 by law enforcement authorities in a high-profile international case involving alleged copyright infringement by users of the service. Some users, which included businesses and individuals who legitimately used the service for non-copyright infringing purposes, instantly lost access to their data and remain engaged in a protracted legal fight seeking its return, which may ultimately not be possible.[29] Although an early edge case, it demonstrates some of the worst-case scenarios that may cause IT professionals to hesitate before migrating to the cloud.

Finally, a number of *uncertainties in law and policy* are perceived as potential inhibitors to cloud growth and to the ability of adopters to use it innovatively. Key issues and topics that apply generally to the cloud environment include jurisdiction (particularly in the international dimension), compliance, transparency, service-level agreements, trade policy, and consumer protection. These and other issues will be discussed in greater detail in later sections.

Over time, many of the obstacles and potential inhibitors may be overcome with new technological solutions or developments in policy. That said, the solutions may require industry actors and policymakers to coordinate actions and work together to creative collaborative solutions.

Implications

Given the relative nascence of the technology and business models, it is difficult to pinpoint the *impact* at this early stage of cloud computing on global businesses and consumers. Markets for cloud computing services have been consistently growing year-over-year. Industry analysts currently estimate that the current global market size for cloud computing services in 2013 will be around US $131 billion, representing an 18.5% growth rate from 2012 figures.[30] The forecast is for continued growth with the market size reaching approximately $210 billion in 2016.

---

[29] *See* Jon Brodkin, "Megaupload data wiped out in 'largest data massacre in Internet history'," *Wired*, June 20, 2013, http://www.wired.co.uk/news/archive/2013-06/20/dotcom-data-deletion; Chloe Albanesius, "Recovering Legitimate Megaupload Files? Good Luck With That," *PC Magazine*, January 20, 2012, http://www.pcmag.com/article2/0,2817,2399162,00.asp.

[30] "Gartner Says Worldwide Public Cloud Services Market to Total $131 Billion," *Gartner*, February 28, 2013, http://www.gartner.com/newsroom/id/2352816; *see also* Louis Columbus, "Gartner Predicts Infrastructure Services Will Accelerate Cloud Computing Growth," *Forbes*, February 19, 2013, http://www.forbes.com/sites/louiscolumbus/2013/02/19/gartner-predicts-infrastructure-services-will-accelerate-cloud-computing-growth/.

The cloud computing industry has caught the attention of governments around the world as a potential *source of economic growth*. Many governments have implemented sophisticated strategies aimed at promoting cloud computing adoption in the private sector, stimulating growth of cloud service providers, and bolstering international competitiveness in the global cloud computing markets.[31] Based on these observations, the outlook from the perspective of governments on the cloud computing industry seems quite positive.

The impact on jobs in the IT sector is somewhat less certain. Although estimates vary, industry commentators believe that a number of traditional IT jobs may be displaced in the short term by cloud computing services, which, as noted earlier, are premised on the outsourcing and streamlining of many of these functions to third party service providers.[32] With this in mind, a number of those displaced jobs may be able to transition into new positions with different responsibilities within the cloud computing industry – by some accounts this is already occurring to an extent. Current signs actually point to a shortage of individuals with the necessary skill sets to work in the cloud computing industry. Overall, the analyst firm IDC estimates that 14 million jobs will be created worldwide by the cloud computing industry by 2015.[33]

2. Law and Cloud Innovation

The previous section framed cloud computing as a technological innovation and innovation-enabling technology, discussed what is driving it, and where it may be heading. This section focuses on how the *legal and regulatory system* interacts with cloud computing by identifying, clustering, and analyzing *reactions* by the legal and regulatory systems in response to the emergence of cloud computing.

Three *caveats* are important against this objective. First, legal and regulatory responses to technological innovation should not be conceived as a simple stimulus-response mechanism, but rather as the product of complex interactions among different social subsystems and forces.[34] Second, bi-directional feedback loops exist between innovative technologies and the legal systems that seek to regulate it. Cloud computing is shaping both the mechanisms policymakers use for detecting pressing policy issues and the regulatory tools with which they may respond.[35]

---

[31] *See* Gasser and O'Brien, "Governments and Cloud Computing."
[32] *See, e.g.*, Ben Brumm, "The Impact of Cloud Computing on IT Jobs," December 2, 2012, http://www.computer.org/portal/web/computingnow/careers/content?g=53319&type=article&urlTitle=the-impact-of-cloud-computing-on-it-jobs.
[33] Microsoft, "Cloud Computing to Create 14 Million New Jobs by 2015," March 5, 2012, http://www.microsoft.com/en-us/news/features/2012/mar12/03-05CloudComputingJobs.aspx.
[34] *See, e.g.*, Charles D. Raab and Paul de Hert, "Tools for Technology Regulation: Seeking Analytical Approaches Beyond Lessig and Hood," in Roger Brownsword and Karen Yeung (eds), *Regulating Technology: Legal futures, regulatory frames and technological fixes* (Oxford: Hart Publishing, 2008), pp. 275 et seq.
[35] *See generally*, Christopher Hood, *Tools of Government* (London: Macmillan, 1983).

Third, cloud computing as a phenomenon has not emerged in a legal and regulatory vacuum. To the contrary, the legal system has in many ways set both the enabling and constraining ground rules for cloud computing, as it has for other technological innovations in the past. IP and contract laws, competition law, and privacy frameworks are just a few examples of the complex and bi-directional relationship between innovation and law.[36] That said, the focus on legal and regulatory responses seem to be a particularly interesting lens in the present context as such reactions are an important factor in the early stage in technology's and market's development.

2.1 Cloud Governance

From a broader *governance* perspective, and before turning to legal and regulatory issues specifically, it is important to emphasize that the "regulatory state" of cloud computing is characterized by four attributes that are also characteristic for other areas of ICT governance:[37]

- *Variety in norms*: A plurality of state actors ranging from national government agencies to supranational institutions with formal rule making capacity have engaged in enacting a diverse set of (partly overlapping or otherwise interacting) norms aimed at regulating certain aspects of the cloud computing phenomenon.[38]
- *Variety in control mechanisms*: In addition to traditional, hierarchical mechanism of control, legal and regulatory approaches to cloud computing include alternative modes of control, such as market regulation, the shaping of social norms, and design requirements.
- *Variety in controllers*: While traditional state regulatory bodies – such as government agencies or courts – continue to play a key role in the context of cloud regulation, important control functions have also been attributed to alternative governance institutions, including standard setting bodies and trade associations.
- *Variety in controllees*: In the cloud computing governance ecosystem, businesses that provide cloud services are the key regulatees. However, a broader range of actors is also relevant to the outcomes of governance efforts, including the government itself – especially where it plays the role of a cloud users.[39]

[36] For an interesting country case study, see Mark Wu, "China Moves to the Cloud," (forthcoming, 2013).
[37] *See generally*, Colin Scott, "Regulation in the Age of Governance: The Rise of the Post Regulatory State," in Jacint Jordana and David Levi-Faur, eds., *The Politics of Regulation: Institutions and Regulatory Reforms for the Age of Governance* (Cheltenham: Edward Elgar, 2004). On the post-regulatory state of cyberspace *see* Andrew D. Murray, "Conceptualizing the Post-Regulatory (Cyber)state," in Roger Brownsword and Karen Yeung, eds., *Regulating Technology: Legal futures, regulatory frames and technological fixes*, (Oxford: Hart Publishing, 2008), pp. 287-315.
[38] For an overview, *see* Gasser and O'Brien, "Governments and Cloud Computing."
[39] On the role of governments in the cloud computing ecosystem, *see* Gasser and O'Brien, "Governments and Cloud Computing."

The following paragraphs zoom in on a subset of issues, norms, mechanisms, and actors that form the governance framework for cloud computing by mapping and discussing the responses of the legal and regulatory system *vis-à-vis* cloud innovation.

2.2 Key Issues

When confronted with technological innovations, legislators and regulators typically use a *range of tools* to detect issues, including instruments of horizon scanning and emerging regulatory issues analysis. Consistent with such approaches, governments around the globe – as well as other players, including trade associations and international organizations – have engaged in analyses of the *risks and challenges* associated with the cloud computing phenomenon.

Shaped by region-specific social, political, and economic factors, a broad range of legal, policy, and regulatory issues have been identified by policymakers and stakeholders. A recent OECD report, for instance, identified the following challenges inherent to cloud computing:[40] spurring the use of cloud computing, standardization, measurement of cloud computing, cloud computing for development, broadband infrastructure, trade and competition implications, tax implications, contractual issues, security and risk management, and privacy. A more extensive list of key issues related to the cloud computing phenomenon emerged from a comparative law and policy review among countries with advanced cloud computing ecosystems.[41] Many of the issues – some of which were mentioned in the previous section – are the product of four basic risk vectors of cloud computing: Outsourcing, centralization, internationalization, and systemic complexity, and can be roughly grouped into vertical and horizontal issues:[42]

Vertical issues

- Data protection: Data protection arguably ranks top among the concerns related to the cloud. The architecture of cloud computing and the sensitive nature of the data stored in such environments lead to concerns regarding individual rights and related safeguards, such as data quality, processing transparency, and international data transfers.
- Data Security: Closely linked to privacy issues are concerns regarding data security, standards, contractual rules, and legal obligations. This includes, for example, digital signature legislation, breach notification laws, laws regulating how data can be stored in the cloud, but also security audit requirements.

[40] OECD, "Internet Economy Outlook 2012," *OECD Publishing* (2012), p. 81-82.
[41] *See* Gasser and O'Brien, "Governments and Cloud Computing"; *see also* Gasser and Palfrey, "Fostering Innovation and Trade."
[42] The following issues list is a quote from Gasser and O'Brien, "Governments and Cloud Computing" which builds upon an initial list discussed in Gasser and Palfrey, "Fostering Innovation and Trade."

- Data retention: Economic regulation as well as national security obligations increasingly require the development, implementation, and operation of retention practices which have to be balanced against civil liberties and other fundamental rights.
- Consumer protection: Concerns about the protection of consumers as users of cloud services include the terms and conditions that apply to such uses, the communication between cloud providers and consumers, and the feasibility of consumer protection law to regulate these relationships that are characterized by information and power asymmetries.
- Intellectual Property: IP often plays an important role in cloud-based business models, ranging from social media to the publication industry. The exploitation of such rights in the cloud environment is in many cases contested. In particular, the low entry barriers for large-scale distribution of copyright protected content causes concerns around piracy on the side of rightholders. IP enforcement mechanisms are also frequently mentioned in cloud policy debates.
- Competition: Given the centralized nature of cloud computing infrastructures, questions of ownership, antitrust, and interoperability have emerged. Issues include among others problems contractual concerns (e.g., *ad hesion* forms of contracts), the lack of portability, and the conflicts between open and closed standards.
- Trade: Restrictive policies – such as the requirement that cloud companies have to register in a given country before they can provide services – that create trade barriers for cloud providers as well as the harmonization of government procurement rules are debated internationally, for instance in the context of multinational agreements such as the Trans-Pacific Partnership (TPP) Agreement, or bilateral trade agreements such as the US-South Korea Trade Agreement.

Horizontal issues

- Jurisdiction, applicable law, enforcement: In order to harness economies of scale, cloud computing often involves the flow of data across jurisdictional boundaries – whether at the local, national, or regional level. From a legal perspective, the global flow of data immediately triggers the questions of jurisdiction, applicable law, and enforcement that are characteristic for Cyberlaw more broadly. In addition, it also raises the question as to what extent a global regulation of cross-jurisdictional data flows would be appropriate; this is relevant, for instance, in the context of the negotiation of the TPP agreement.
- Compliance: Cloud computing providers need not only to obey to general laws, but also to comply with quickly expanding and often very detailed sector-specific laws (e.g., regarding financial, educational, or health data) and master the interplay among them, especially where such laws and regulations vary across jurisdictions.
- Transparency: Transparency and clarity are central cross-sectional concerns identified both regarding contractual arrangements as well as regulatory approaches to cloud

computing as a technologically, organizationally, and economically complex phenomenon.

- Responsibility and liability, including cybercrime: Closely linked to transparency and an inherent element for providing an appropriate legal and regulatory framework for cloud computing is the clarification of areas of responsibility for all parties involved. Instruments range from traditional approaches (criminal law, civil liability, and risk insurance) to concepts such as corporate social responsibility.
- Infrastructure: Especially in emerging economies, but to a certain extent also in countries with advanced cloud strategies such as the US and the EU, the availability and competitiveness of infrastructure that supports the digital economy and cloud computing has been identified as an important policy topic, as the often controversial discussions around national broadband plans illustrate.

Vertical and horizontal issues are analytically distinct categories, but often *interact* with each other. The interplay between the privacy and transparency debate in the EU is illustrative in this respect, where the lack of transparency in contracts about responsibilities and privacy-relevant practices has been identified among the factors that might further increase privacy vulnerabilities for consumers of cloud services.[43]

3.3 Response Patterns

Across jurisdictions, many of the issues mentioned in the previous paragraphs have begun stimulating a series of *specific responses* by the legal and regulatory system.[44] The *activation* of law and regulation as well as the type of responses triggered are the result of a complex set of interactions among different social subsystems, institutions, and forces.[45] They are also shaped in important ways by context and culture.[46] Despite such context-specificity, however, two *basic response patterns* and associated activation mechanisms can be distinguished when legislators and regulators are confronted with a technology-based innovation phenomenon such as cloud computing: "subsumption" and the creation of new law.[47]

Subsumption

The default approach of law to technological innovation in the Western world can be described as a mode of subsumption, where the legal system – once activated by one of the involved actors

[43] *See* Gasser and O'Brien, "Governments and Cloud Computing."
[44] *Id*.
[45] *See, e.g.*, Charles D. Raab and Paul de Hert, "Tools for Technology Regulation: Seeking Analytical Approaches Beyond Lessig and Hood," in Roger Brownsword and Karen Yeung (eds), *Regulating Technology: Legal futures, regulatory frames and technological fixes*, (Oxford: Hart Publishing, 2008), pp. 275 et seq.
[46] *Id*.
[47] *See* Burkert and Gasser, "Regulating Technological Innovation."

– *applies old rules* to a perceived new problem triggered by an innovative technology.[48] It relies on a spectrum of instruments, ranging from contractual agreements and best practices to litigation with the involvement of courts.

In the cloud context, *contracts* have played a particularly important role in embracing (and absorbing) some of the challenges associated with the technological innovation. In the first phase, cloud providers and customers have addressed core issues using contractual agreements to identify and allocate risks and responsibilities and create enforcement mechanisms where existing rules are inadequate. Such innovation-driven contractual adaptations include, for instance, specific rules regarding data privacy and security, data breach notification, e-discovery, or service level agreements, to name just a few. Driven by negotiations and market developments, such contract terms for cloud computing services continue to evolve with the issues and related market developments.[49]

Highlighting the important role of contracts – as well as their complexity, legal uncertainty, and the power asymmetries among the parties to an agreement – various stakeholders have started to work towards *best practice models*, which mark the second phase of using contracts as a way to legally embrace the effects of cloud innovation. For instance, the US CIO Council, in collaboration with other government units, developed guidelines for effective cloud computing contracts for the federal government.[50] More broadly, the European Commission announced the development of "safe and fair contract terms and conditions" as part of its cloud strategy[51] and recently set up an expert group on this topic.[52]

Following a well-known pattern,[53] the *court system* has become involved as part of the legal system's response system in instances where cloud computing as an innovation-enabling technology has led to specific disruptive effects for incumbent business models. Typically, the first wave of innovation-driven disputes include intellectual property issues, where the courts are asked to clarify as to what extent existing legal norms and doctrines apply to the new phenomenon. With respect to cloud computing, cases such as Cablevision I and II in the US, a dispute about the applicability of copyright law to a innovative cloud-based remote storage DVR

---

[48] *Id*.
[49] *See* W. Kuan Hon, Christopher Millard, and Ian Walden, "Negotiating Cloud Contracts: Looking at Clouds from Both Sides Now," 16 *Stanford Tech Law Review* 81 (2012), http://stlr.stanford.edu/2013/01/negotiating-cloud-contracts/; *see also* William R. Denny, "Survey of Recent Developments in the Law of Cloud Computing and Software as a Service Agreement," 66 *Business Lawyer* 237 (November 2010).
[50] US CIO Council and Chief Acquisition Officers Council, "Creating Effective Cloud Computing Contracts for the Federal Government," (February 24, 2012), https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf.
[51] *See, e.g.*, European Commission (EC), "Unleashing the Potential of the Cloud in Europe," COM(2012) 529, Brussels, 27.9.2012, http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf.
[52] EC, "Cloud Computing Contracts," http://ec.europa.eu/justice/contract/cloud-computing/index_en.htm.
[53] Deborah L. Spar, *Ruling the Waves. From the Compass to the Internet, a History of Business and Politics along the Technological Frontier* (New York: Harcourt, Inc., 2001).

technology and television broadcasts,[54] or the MYUTA case, which involved a copyright dispute over cloud-based music storage for mobile phones in Japan, exemplify how the court systems are used as response mechanisms. A second wave of litigation has emerged around data breaches and privacy issues, as illustrated by recent private lawsuits and regulatory investigations involving cloud providers such as Google, Dropbox, and Facebook.[55]

Legal innovation

A second basic response mode of the legal system *vis-à-vis* technological innovation is the *creation of new law* or *legal innovation*, which can either be induced by courts via new precedent or by legislators via statutory or regulatory intervention.[56] Over the past two years, various aspects of the multi-faceted phenomenon cloud computing have caught the attention of lawmakers and regulators, both at the national and international level. As a result of ongoing debates about the risks and opportunities of cloud computing, new proposals for amendments to existing laws, new legislation and regulations have emerged. Proposed laws in the US and the EU, such as the Cloud Computing Act of 2012,[57] updates to the Electronic Communications Privacy Act,[58] and proposed revisions of the privacy legislation in the EU[59] represent a few examples in this category.

---

[54] *Twentieth Century Fox Film Co. v. Cabelvision Systems Corp.*, 478 F.Supp.2d 607 (S.D.N.Y 2007) ("Cablevision I"); *Cartoon Network LP v. CSC Holdings*, 536 F.3d 121 (2d Cir. 2008) ("Cablevision II").

[55] *See In the Matter of Google, Inc., a corporation*, FTC Complaint ("Google I"), http://ftc.gov/os/caselist/1023136/111024googlebuzzcmpt.pdf; *United States v. Google, Inc.*, Stipulated Order for Permanent Injunction and Civil Penalty (N.D. Cal. June 2012), http://www.ftc.gov/os/caselist/c4336/120809googlestip.pdf; *United States v. Google, Inc.*, 12-cv-04177 (N.D. Cal. Aug. 8, 2012) ("Google II"), http://ftc.gov/os/caselist/c4336/120809googlecmptexhibits.pdf; *In the Matter of Facebook, Inc.*, a corporation, FTC Decision and Order, no. C-4365 (July 27, 2012), http://www.ftc.gov/os/caselist/0923184/120810facebookdo.pdf; *see also* Ryan Singel, "Dropbox Lied to Users About Data Security, Compliant to FTC Alleges," *Wired*, May 13, 2011, http://www.wired.com/threatlevel/2011/05/dropbox-ftc/.

[56] A prominent example of court-induced innovation in the information and technology space is the *Grokster* ruling, where the US Supreme Court introduced the inducement rule into copyright law. *Metro-Goldwyn-Mayer v. Grokster*, 545 U.S. 913 (2005). An example of a legislative response in the US is the Digital Millennium Copyright Act (DMCA), which was amended the existing Copyright Act to address issues related to the sharing of Copyrighted materials on the Internet. Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, 112 Stat. 2860. *See also* Urs Gasser and John Palfrey, "Breaking Down Digital Barriers: When and How ICT Interoperability Drives Innovation," *Berkman Center Research Publication No. 2007-8*, (2007), http://ssrn.com/abstract=1033226.

[57] Cloud Computing Act of 2012, S. 3569 ,112th (2011-2012), http://beta.congress.gov/bill/112th/senate-bill/3569/text.

[58] Often criticized for its age and ill-application to new technology, the Electronic Communications Privacy Act (ECPA) provides a series of protections against access by the government of information related to private communications facilitated by through third-party mediums. The Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522, 2701-2712. Recently, legislators have introduced new proposals to updates these laws in response to technological developments like cloud computing. *See, e.g.*, Electronic Communications Privacy Act Amendments of 2013, S. 607, 113th Cong. (2013-2014), text available at http://beta.congress.gov/bill/113th-congress/senate-bill/607.

[59] EC, Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, WP 196 (July 1, 2012), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

The creation or proposal of new laws typically gain high public visibility, particularly in the case where a law would engender sweeping changes to the existing regulatory structure. The creation of new law faces a series of challenges, as discussed further below, including the risk of unintended consequences, and can often be as time consuming as the subsumption approach. Concurrent to the high-visibility legislation and regulation processes, a more *gradual adaptation* processes might take place, which over time may also culminate in structural changes in law. Various bilateral and emerging plurilateral trade agreements such as the Trans Pacific Partnership (TPP) agreement with cloud-relevant provisions might be examples for such adaptation processes that are often at least initially below the public's radar.

2.4 Functions

In the context of information and communication technologies, law has been traditionally used to *constrain* behaviors: "Law (...) directs behavior in certain ways; it threatens sanctions ex post if those orders are not obeyed."[60] Legal norms that impose liability for certain behaviors are prime examples of law functioning as a constraint. For example, if an individual willfully distributes a copyrighted work in the US without authorization, she is subject to statutory damages.[61] This restrictive understanding of law has also shaped the notion of "code as law," where software constrains user behavior ex ante, as embedded in hardware or software.[62]

However, hard and soft law can also serve the role of an *enabler*, where it opens up spaces for technological and social innovation and interaction, enables transactions, and supports various modes of production and collaboration. Contract law is an example of enabling law, as it allows innovators to privately stipulate the "ground rules" of transactions. Other examples include intellectual property and trade laws, as they provide incentives to innovate via baseline legal protections, to name just two other innovation-relevant examples.

The third basic function of law in the innovation context is its *leveling power*. In this function, the law aims to right a normative or market imbalance in power. Competition law aimed at protecting consumer welfare is a case in point. It involves the regulation of competitors within an economy in order to establish a level playing field by controlling the creation of monopolies and oligopolies. Model contract laws aimed at reducing asymmetries between contracting parties or legal approaches in support of standard setting in the technical field are other illustrations where the legal system serves a leveling function in innovation-relevant spaces.

[60] Lawrence Lessig, "The New Chicago School," 27 *Journal of Legal Studies* 661, 662 (June 1998).
[61] 17 U.S.C. § 504.
[62] Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 2000).

All three functions of law can also be observed overlapping in the cloud computing context. Indeed, as already noted above, cloud computing as an innovative technology has emerged based on a sophisticated set of general laws and regulations that enable – and at times foster – technological innovation. For example, the availability of contract law and corresponding enforcement mechanisms is key to create for enabling a viable transactional environment where cloud provider and users can engage in privately ordering. Licensing arrangements enable the transfer of intellectual assets and knowledge between cloud computing developers. Governmental support of standard-setting initiatives such as the National Institute for Standards and Technology (NIST) in the US both enables an interoperable market place and levels imbalances created by proprietary standards.[63] In the EU, the proposed Regulation on a Common European Sales Law aims to foster cross-jurisdictional transactions in the cloud age is another examples leveling powers.[64] Finally, several recently proposed laws are aimed at constraining the behavior of cloud providers with respect to the collection, processing, and use of personal information.[65]

2.5 Modes

The cloud computing *governance mix* includes various modes of regulation, including hierarchical, competition-based, community-based, and design-based mechanisms of control.[66] Looking at the main approaches by which *legislators and regulators* have started addressing risks and challenges associated with cloud computing, a recent survey of selected jurisdictions identified three modes of response: top-down approaches where the government directly seek to intervene into the cloud computing environment, processes of co-regulation, and finally mechanisms of industry self-regulation.[67] Examples for each category include the following:

- *Direct intervention*: Proposed legal and regulatory interventions aimed at protecting users' privacy in the cloud computing environment are illustrative of top-down approaches by the government. Examples include the proposed amendments to the US Electronic Communication Privacy Act (ECPA) as well as the recently proposed privacy regulations in the EU that are at least in part targeted at cloud service providers.

[63] Cloud Computing Program, http://www.nist.gov/itl/cloud/
[64] EC, "Regulation of the European Parliament and of the Council on a Common European Sales Law," Brussels, 11.10.2011, COM(2011) 635 final, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0635:FIN:en:PDF.
[65] In the US, *see, e.g.*, H.R. 5777, 111th Cong. 2d Sess. (July 19, 2010), http://www.gpo.gov/fdsys/pkg/BILLS-111hr5777ih/pdf/BILLS-111hr5777ih.pdf; in the EU *see, e.g.*, EC, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation," Brussels 25.1.2012, COM(2011) 11 final, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.
[66] On hybrid regulation, *see, e.g.*, Andrew Murray and Colin Scott, "Controlling the New Media: Hybrid Responses to New Forms of Power", 65 *Modern Law Review* 491 (2002), available at: http://ssrn.com/abstract=317844.
[67] *See* Gasser and O'Brien, "Governments and Cloud Computing."

- *Co-regulation*: Some of the government facilitated standard-setting initiatives in the US and the EU are examples of co-regulation, where industry players, governments, and other stakeholders act in concert to address a specific regulatory issue – for instance data security challenges or interoperability issues.
- *Self-regulation*: In this mode, the cloud industry rather than the government is engaged in main components of regulation (while the government might still be involved in others). Self-regulation has been proposed, for instance, in the context of the development of model contract terms in the EU.

A comparative analysis of the different modes of law and regulation used across a number of jurisdictions indicates that the modalities of regulation are typically considered on by legislators and regulators on an issue-by-issue basis and are not the product of a more general vision regarding the shape of a cloud computing governance model.[68] However, the legal culture and framework within a country or region shapes both the default mode of regulation and blended approaches. The EU, for instance, seems to prefer direct interventions concerning privacy challenges while considering co-regulation or self-regulatory initiatives with regard to contractual issues such as standard terms.[69]

2.6 Strategies

Legislators and regulators have a number of macro-regulatory strategies available when pursuing particular policy objectives and addressing legal and regulatory issues in complex systems such as innovative high-tech environments.[70] The legal and regulatory "toolbox" includes (general) instruments such as command-and-control, incentive-based regulation, market-harnessing controls, among others. Some of these strategies have proven to be particularly helpful when regulating under conditions of uncertainty, where outcomes of interventions are often unpredictable.[71]

A series of country case studies suggests that legislators and regulators have pursued a diverse set of strategies available in the toolbox when addressing challenges associated with cloud computing as a technological innovation and innovation-enabling technology.[72] A comparative review of these cases suggests that the use of the respective instruments in the cloud computing context is closely linked to the role the government seeks to play and, connected with it, the

[68] *Id*.
[69] *Id*.
[70] *See, e.g.*, Robert Baldwin and Martin E. Cave, *Understanding Regulation: Theory, Strategy, and Practice* (Oxford: Oxford University Press, 1999).
[71] *See, e.g.*, Andrew D. Murray, "Conceptualizing the Post-Regulatory (Cyber)state," in Roger Brownsword and Karen Yeung (eds), *Regulating Technology: Legal futures, regulatory frames and technological fixes* (Oxford: Hart Publishing, 2008), p. 291.
[72] *See* Gasser and O'Brien, "Governments and Cloud Computing."

rationale for and modes of regulation discussed in the previous paragraphs.[73] Examples include the following:[74]

- *Command and control*: Direct interventions to exercise control by imposing rules or standards backed-up by sanctions. Examples: Cloud Computing Act of 2012; revision of privacy legislation to ensure privacy safeguards for cloud environment; registration requirements for cloud providers.
- *Incentive-based:* Influence behavior by imposing negative or positive taxes, deploying grants or subsidies from the government. Example: Use of procurement power to stimulate growth of cloud ecosystem by supporting SMEs.[75]
- *Market-harnessing:* Regulatory interventions to sustain certain levels of competition that benefits users and the public. Example: Competition law and antitrust investigations triggered by the market share and/or certain practices of cloud service providers.[76]
- *Disclosure:* Interventions aimed at structuring the disclosure of information to provide consumers with sufficient data on products and services. For example, data breach notification laws.[77]
- *Rights and liability:* Allocate rights and liability to encourage socially desirable behavior. Example: Sector specific liability laws applicable to cloud solutions, e.g., health or financial markets.[78]

From the perspectives of legislators and regulators, cloud computing is still a nascent and evolving technology. Against this backdrop, it is arguably premature to identify regulatory best practice models and ideal regulatory modes. Although, it is worth noting that a trade association recently published a helpful normative benchmark regarding cloud regulatory performance across a series of countries.[79] From a more anecdotal perspective, the initial set of country case studies suggests that command-and-control, disclosure, and rights and liability schemes currently play a more important role than other strategies when dealing with risk and challenges associated

---

[73] *Id*.
[74] *Id*.
[75] This is a key feature of the UK Government's ICT and cloud strategies, which emphasize that "the Government will also put an end to the oligopoly of large suppliers that monopolise its ICT provision" and "remove barriers to allow SMEs, the voluntary and community sector and social enterprise to participate in the ICT marketplace." UK Government, Cabinet Office, "Government Cloud Strategy," 2011, pp. 8-10, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/85982/government-cloud-strategy_0.pdf.
[76] Google, for example, has been the target of several antitrust investigations involving regulators in the US and Europe. *See, e.g.*, James Kanter and Claire Miller, "In European Antitrust Fight, Google Needs to Appease Competitors," *New York Times*, July 17, 2013, http://www.nytimes.com/2013/07/18/technology/europe-wants-more-concessions-from-google.html; Edward Wyatt, "F.T.C. Is Said to Begin a New Inquiry on Google," *New York Times*, May 24, 2013, http://www.nytimes.com/2013/05/25/technology/ftc-said-to-have-begun-new-inquiry-on-google.html.
[77] *See, e.g.*, Paul Schwartz, "Information Privacy in the Cloud," 16 *University of Pennsylvania* 1623 (May 2013).
[78] *See, e.g.*, J. Nicholas Hoover, "Compliance in the Ether: Cloud computing, data security and business regulation," 8 *Journal of Business & Technology Law* 255 (2013).
[79] *See, e.g.*, "2013 BSA Global Cloud Computing Scorecard," http://cloudscorecard.bsa.org/2013/ .

with cloud computing technology.[80] Based on experiences in other areas of technology law and policymaking, one might expect that additional instruments – for instance, insurance frameworks – will be applied to the cloud innovation phenomenon over time.[81]

3. Challenges

The previous section tracked, clustered, and mapped responses by the legal and regulatory system in response to cloud computing as an example of an innovative and innovation-enabling technology. Throughout the discussion, it has become clear that lawmakers and regulators will have to make many choices in response to the cloud computing phenomenon – including the choice to respond to certain regulatory issues (such as, for instance, privacy, interoperability, etc.) or not to respond at all. This section identifies a selection of challenges involved in making such choices about legal and regulatory interventions, strategies, tools, and the like with regard to cloud innovation.

It is important to note that several other challenges could be added to the list below, but the following selection, clustered into three chronologically staggered phases (the conceptual, implementation, and assessment phases) is at least indicative of the complexity regulators face when aiming to regulate an innovative technology such as cloud computing. While not all of the challenges are specific to technology regulation, several of problems are amplified when applied to a dynamic technological environment.

3.1 Conceptual phase

Conceptual challenges describe basic "horizontal" challenges legislators and regulators are confronted with when considering the regulation of a technological innovation. In the cloud context, three sets of challenges have become visible based on a series of in-depth country case studies: justification of law and regulation, trade-offs between policy objectives, and conflicts among the different roles governments play.[82]

Justification

Governments have a range of mechanisms available to detect legal and regulatory issues related to cloud innovation. What issue makes it onto the legal and regulatory agenda further depends on the political economy in which a technology such as cloud computing emerges and diffuses and, accordingly, may vary across countries. The identification of legal and regulatory issues

[80] Gasser and O'Brien, "Governments and Cloud Computing."
[81] *Id*.
[82] *See* Gasser and O'Brien, "Governments and Cloud Computing."

through mechanisms such as horizon scanning typically includes an assessment of the need for intervention, for instance in case of a market failure. The justification of law and regulation in the cloud innovation environment is complicated by the fact that there is plenty of anecdotal evidence but not much empirical data available on its precise impact in a given area of concern. The data challenge together with the other "soft" factors suggests that problem solving at least in the nascent stages of cloud innovation is often more based "on intuition, experience, tradition, faith and serendipity" as well as "a mixture of chance and trial and error" rather than a rational choice model.[83]

Trade-offs

Another familiar conceptual challenge in the context of technology regulation concerns tensions and, in some cases, trade-offs among values and underlying policy objectives. In the case of cloud innovation, such trade-offs have become particularly visible where lawmakers and regulators seek to establish or strengthen frameworks aimed at enhancing consumer trust in cloud computing technology. For instance, updating existing privacy legislation to make it fit for the cloud age while simultaneously pursuing national security interests through massive surveillance programs, which heavily target cloud computing services and providers and – at least as a matter of perception – are diametrical to regulators' efforts to promote trust in cloud computing.[84] At least in sensitive areas such as national security, facilitation mechanisms that could help negotiating and bridging such value conflicts and regulatory trade-offs are not yet developed, as the case of cloud innovation suggests.

Role conflicts

A third conceptual challenge identified based on a previous analysis of the role of governments (broadly defined) in the cloud computing environment relates to role conflicts. An extensive review of advanced cloud computing strategies adopted by governments around the world suggests that they typically play more than one role in relation to cloud innovation.[85] Simultaneously, governments may play the (partly overlapping) role of users, regulators, coordinators, promoters, researchers, and service providers.[86] Both conceptually and in at the implementation level, the multitude of roles played can result in role conflicts that need to be addressed and managed. With respect to cloud innovation, law, and regulation, conflicts might

[83] *See* Christopher Hood, *Tools of Government*, (London: Macmillan, 1983), p. 135-137; *see also* Charles D. Raab and Paul de Hert, "Tools for Technology Regulation: Seeking Analytical Approaches Beyond Lessig and Hood," in Roger Brownsword and Karen Yeung (eds), *Regulating Technology: Legal futures, regulatory frames and technological fixes*, (Oxford: Hart Publishing, 2008), at p. 278.
[84] *See* Jordan Novet, "PRISM could foil the public-cloud campaign, and private clouds may lie in crosshairs," *GigaOm*, June 17, 2013, http://gigaom.com/2013/06/17/prism-could-foil-the-public-cloud-campaign-and-private-clouds-might-lie-in-crosshairs/.
[85] Gasser and O'Brien, "Governments and Cloud Computing."
[86] *Id*.

for instance arise between regulatory compliance (government as regulator) and cloud-first strategies (government as user). Tension areas between the roles as regulator and promotional activities for industry are another illustration. The lack of protective legislation in some countries, for example, might discourage private sector adoption both domestically and internationally. Conversely, regulatory requirements in sensitive areas such as health or finance may be tightened in the cloud environment and discourage cloud adoption in the private sector.[87]

3.2 Implementation phase

Interacting with conceptual challenges, a comparative analysis of legal and regulatory responses to cloud innovation suggests a series of implementation problems, some of which have already been discussed in the previous section. Three such challenges seem particularly noteworthy: problems related to definitions, timing issues, and the challenge of appropriate tool selection.

Metaphors and definitions

When confronted with innovative technologies, lawmakers and regulators typically use analogies or metaphors to understand the new phenomenon. Analyses of the use of metaphors in the context of Internet regulation suggest how metaphors can shape regulatory thinking at the conceptual level and influence approaches at the implementation level.[88] Similarly, the definitions that are used to describe the new phenomenon or certain aspects of it can influence approaches. Given the high degree of technicality and the fluidity in the cloud computing environment, legislators and regulators may not develop their own technical definitions, but instead defer to definitions set forth by standard setting organizations.[89] One example where this occurred in the US was the proposed Cloud Computing Act of 2012, which sought to use NIST cloud computing definitions to establish a new type of violation involving unauthorized access to computer systems in the Computer Fraud and Abuse Act.[90] The proposal was met with criticism

---

[87] *Id*.
[88] *See, e.g.*, Alfred C. Yen, "Western Frontier or Fuedal Society?: Metaphors and Perceptions of Cyberspace," 17 *Berkeley Technology Law Journal* 1207 (Fall 2002), available at: http://www.law.berkeley.edu/journals/btlj/articles/vol17/Yen.stripped.pdf; Annete N. Markham, "Metaphors Reflecting and Shaping the Reality of the Internet: Tool, Place, Way of Being," (2003), http://markham.Internetinquiry.org/writing/MarkhamTPW.pdf; David J. Gunkel, "The Rule Metaphor: Prolegomena to Any Future Internet Regulation," 8 (2) The Electronic Journal of Communication (1998), http://www.cios.org/EJCPUBLIC/008/2/00826.HTML; Kristen Osenga "The Internet is not a Super Highway: Using Metaphors to Communicate Information and Communications Policy," 3 *Journal of Information Policy* 30 (2013), http://jip.vmhost.psu.edu/ojs/index.php/jip/article/download/117/72.
[89] Gasser and O'Brien, "Governments and Cloud Computing."
[90] Cloud Computing Act of 2012, S. 3569 ,112th (2011-2012), http://beta.congress.gov/bill/112th/senate-bill/3569/text. The Computer Fraud and Abuse Act is the primary US federal law criminalizing unauthorized access to and damage to protected computer systems. 18 U.S.C. § 1030. The NIST definitions were not intended to be used in legislative drafting. *See* Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing," US National Institute for Standards and Technology (NIST), Special Publication 800-145, September 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

from legal scholars for its definitional imprecision.[91] Such definitional challenges are of course not new, but might be amplified in regulatory environments such as cloud computing, given its relatively complex and layered technical characteristics described in Section 1.

Timing

Related to the previously mentioned challenge to determine the need for intervention through law and regulation is the question *when* is it best to intervene? As in other rapidly changing areas of technology, determining the right timing is a critical factor in the cloud computing environment. For instance, lawmakers and regulators need to carefully consider timing issues when attempting to strike a balance between the creation of an enabling innovation environment for cloud innovators on the one hand and safeguarding users on the other. Ideally, the relevant actors use a broad range of analytical tools in this process, including a multi-factor analysis, which encompasses among other things an assessment of the maturity of the technology, standards, and markets with strong network effects.[92] In addition, it is important that lawmakers and regulators monitor how cloud technology, markets, strategies, and adoption change over time and affect the need for intervention or the effectiveness of the legal and regulatory instruments.

Tool Selection

A key implementation challenge once lawmakers and regulators have decided to respond to a particular issue associated with a new technology – beyond the "background rules" that are already in place when the technology emerges – is to select the appropriate tool that is best suited to solve a given regulatory issue or legal problem.

The lack of data makes it difficult to understand the contours of the problem in detail; multi-faceted interoperability issues in the cloud environment are one example that illustrate how nuanced problem description can get.[93] Conversely, on the side of remedies, the matchmaking process between problem and tool is complicated by the fact that data about the performance of a given tool in a specific context is rarely available in advance. The use of a particular tool should align with the mix of with other policy instruments chosen by regulators. Necessarily, selecting the right tools requires consideration of a number of factors including the political, technical, market contexts, and other factors that need to be taken into account.[94]

---

[91] Eric Goldman, "The Proposed 'Cloud Computing Act of 2012,' and How Internet Regulation Can Go Awry," *Technology & Market Law Blog*, October 11, 2012, http://blog.ericgoldman.org/archives/2012/10/the_proposed_cl.htm.
[92] *Id*.
[93] *See* John Palfrey and Urs Gasser, *Interop: The Promise and Perils of Highly Interconnected Systems* (New York: Basic Books, 2012); Gasser and Palfrey, "Fostering Innovation and Trade."
[94] *See, e.g.*, Charles D. Raab and Paul de Hert, "Tools for Technology Regulation: Seeking Analytical Approaches Beyond Lessig and Hood," in Roger Brownsword and Karen Yeung (eds), *Regulating Technology: Legal futures,*

3.3 Assessment phase

A third category of challenges emerges during what one might call the "assessment phase," that is after a particular legal or regulatory intervention has taken place and when looking at the effects of such interventions. Again, the three problems listed below interact with the previous phases and challenges and represent only a subset of issues.

Measures of success

Assessment challenges arise at multiple levels. For instance, there is no general agreed-upon and stable set of criteria to evaluate the performance of the various tools lawmakers and regulators have in their toolbox across different regulatory contexts. In some instances, criteria might focus on dimensions such as coerciveness, directness, automaticity, and visibility.[95] In other contexts criteria such as effectiveness, efficiency, and flexibility might take center stage.[96] And perhaps more often than not, the use of helpful and consistent benchmarks to evaluate regulatory instruments and their performance change over a period of time or do not get much attention at all. Beyond instruments, it is often not clear what success means with respect to the outcomes of technology regulation. Consider, for instance, interventions aimed at addressing data breach problems in the cloud computing environment, where it is far from obvious what constitutes success. The complexity of such normative questions regarding the result of legal and regulatory interventions only increases where multiple tools are at work simultaneously, or where a variety of instruments are used to pursue different and sometimes even competing policy objectives, as discussed before. The controversial debates about the trade-off between privacy and national security in the cloud age are illustrative in this respect.

Unintended consequences

Regulation in general and regulation of innovative technologies in particular can lead to unintended consequences.[97] A prominent example of this type of challenge are side-effects of the Digital Millennium Copyright Act in the US, which was enacted – among other things – to

---

regulatory frames and technological fixes, (Oxford: Hart Publishing, 2008), pp. 275 et seq. For a general framework of the politics of policy instrument selection *see* B. Guy Peters, "The Politics of Tool Choice," in Lester M. Salamon, ed., *The Tools of Government: A Guide to the New Governance* (New York: Oxford University Press, 2002), pp. 552-564.

[95] *See, e.g.*, Lester M. Salamon, "The New Governance and the Tools of Public Action: An Introduction," in Lester M. Salamon, ed., *The Tools of Government: A Guide to the New Governance*, *The Tools of Government: A Guide to the New Governance* (New York: Oxford University Press, 2002), pp. 22-23.

[96] In the context of interoperability (as a concrete problem context), *see, e.g.*, Gasser and Palfrey, "Breaking Down Digital Barriers: When and How ICT Interoperability Drives Innovation," *Berkman Center Research Publication No. 2007-8*, (2007), p. 22, http://ssrn.com/abstract=1033226.

[97] For a thorough discussion of unintended consequences in the context technology regulation, *see* Daniel Gervais, "The Regulation of Inchoate Technologies," 47 *Houston Law Review* 665 (Fall 2010).

provide additional layers of protection of copyrighted works, but has been arguably used in ways unintended by the legislator.[98] The controversy around the proposed Cloud Computing Act of 2012 points out that unintended consequences are also lurking in the background. Critics of used the bill as a an "excellent case study of how even well-meaning legislators can botch Internet regulation."[99] The high complexity of the cloud computing ecosystem increases the likelihood that regulatory interventions will cause unanticipated effects, according to the law of unintended consequences.[100]

Ability to learn

Regulating a bleeding-edge technology, like cloud computing, requires an assumption of uncertainty. The cloud computing legal and regulatory environment is characterized by high degrees of technical complexity and fast changing market conditions, among other things. These overall characteristics in combination with the conceptual, implementation, and assessment phase challenges suggest that regulatory systems should incorporate feedback loops, and mechanisms of self-assessment and correction. The design of such mechanisms of learning is far from trivial. Sunset clauses, periodic reviews, and consultation mechanisms are some of the familiar approaches, but often these instruments are either relatively crude or not well-calibrated to the speed of evolution of high technology and corresponding market dynamics, as for instance the long review cycles of technology-relevant European Union legislation demonstrate.[101]

4. Interface Design

The previous section has identified some of the key challenges lawmakers and regulators face when considering responses to innovative technologies such as cloud computing. Approaches to each of these challenges – whether more technical or normative in nature – need to be developed separately, but also considered in the context of their potential interplay.

A possible approach that might be helpful across these areas is the improvement of *interface design*. The envisioned design improvements of technical, organizational, and human interfaces would be aimed at *enhancing interoperability* across different components of the legal and

[98] Electronic Frontier Foundation, "Unintended Consequences: Fifteen Years under the DMCA," (March 2013), https://www.eff.org/press/releases/fifteen-years-dmca-abuse.
[99] *See, e.g.*, Eric Goldman, "The Proposed 'Cloud Computing Act of 2012,' and How Internet Regulation Can Go Awry," *Technology & Market Law Blog*, October 11, 2012, http://blog.ericgoldman.org/archives/2012/10/the_proposed_cl.htm.
[100] *See, e.g.*, Rob Norton, "Unintended Consequences," *The Concise Encyclopedia of Economics 2d Edition*, http://www.econlib.org/library/Enc/UnintendedConsequences.html. *See also* Daniel Gervais, "The Regulation of Inchoate Technologies."
[101] *See generally*, Jacob E. Gersen, "Temporary Legislation," 74 *University of Chicago Law Review* 247 (Winter 2007).

regulatory system on the one hand and between the legal and regulatory realm and phenomenological (technical, economic, cultural, etc.) spaces in which innovation takes place on the other hand.

Interface design needs to be advanced at three conceptual layers. First, at the *data layer*, in order to increase the legal and regulatory system's capacity to receive and process data about a given technological innovation and its effects on society. An improved interface between technology-relevant research and law and regulation would be a key component of such a system, building and expanding upon existing frameworks of technology impact assessment and foresight analysis.[102] The advancement of Internet science and the attempt to translate research data into manageable inputs that are relevant for regulators is an important example along these lines.[103]

Improved interfaces are not only necessary at the data level, but also with respect to the normative spheres, at the *value layer*. The systematic exchange of information about values is important across the various components within the legal and regulatory system, as the above-mentioned problem of regulatory trade-offs illustrates. Strategic mechanism that enable higher levels of interoperability with regard to normative issues are equally important across systems, for instance between the regulatory and the cultural system. The controversy about national security interests and the acceptable degree of government surveillance in the cloud is a case in point in this respect. Lastly, improved interfaces are required across different legal and regulatory systems, particularly across jurisdictions. In cloud computing environments, for instance, data typically flows across jurisdictions and is allocated dynamically depending on the available processing resources, which enables efficiency gains and cost savings. This feature of cloud innovation requires mechanisms – membranes of sorts – to facilitate and bridge between different normative viewpoints on a broad range of issues. Processes established in the context of the EU-US Transatlantic Trade and Investment Partnership might contribute to such an enhanced interface function, to name just one cloud-relevant example.

Finally, enhanced interfaces would benefit information exchange at the *level of design* of legal and regulatory interventions. Specifically, enhanced feedback loops between the use of particular regulatory strategies and instruments and performance measurement and evaluation would greatly improve the effectiveness and efficiency of technology regulation. Interface design improvements are also relevant beyond the toolbox of law and regulation discussed in this paper when looking at governance mechanisms more broadly. To create an effective blend of governance instruments, including architecture, social norms, and markets, requires interaction

[102] *See, e.g.*, Torsti Loikkanen, Pirjo Kutinlahti, and Annele Eerola, "Towards an Integrated Framework of Impact Assessment and Foresight Studies in Innovation Policy Analysis," *The Second Seminar on Future-oriented Technology Analysis, Seville* (August 21, 2006).

[103] For example, the European Commission has funded and hosted conferences and other events that aim to bring together scholars, policymakers, and practitioners to foster a dialogue on computer science, economics, law, epistemology, and other disciplines. *See, e.g.*, *The 1st International Conference on Internet Science*, held April 10-11, 2013, Brussels, Belgium, http://Internetscienceconference.eu/.

among the different approaches and fine-tuned coordination processes among the respective actors.[104]

5. Conclusion

Looking at cloud computing as a rich case study of a technological innovation and innovation-enabling technology with significant societal implications, this paper identifies and discusses several dimensions of the interplay between innovation, law, and regulation. At the most basic level and synthesizing a previous review of various country studies on government approaches to cloud computing, it confirms a *bidirectional relationship* between law/regulation and innovation.[105] On the one hand, the legal and regulatory system typically shapes the emergence and evolution of innovative technologies, for instance through IP law, contract law, antitrust law, etc. On the other hand, innovative technologies in general and novel technologies with disruptive effects in particular typically trigger an activation of the legal and regulatory system.

Focusing on the instances in which the legal and regulatory system has been activated, the paper briefly sketches the regulatory state of cloud computing and distills a series of *legal and regulatory issues* that have emerged across various jurisdictions in a complex process of issue detection and analysis by lawmakers and regulators. In this context, a basic *response pattern* framework is useful for clustering specific legal and regulatory interventions in the cloud computing space, illustrating the respective roles of private actors and courts in applying old rules to the new phenomenon through subsumption as well as those of governments in creating new regulation.

The analysis of legal and regulatory responses in the cloud innovation context confirms a set of distinct *functions* of regulation, including a constraining, enabling, and leveling function and, by applying general frameworks from regulation theory, identifies a set of well-established modes of law and regulation, including top-down regulation, processes of co-regulation, and self-regulation with corresponding regulatory strategies, such as command and control and incentive-based regulation.

Across these areas and activities, lawmakers and regulators are confronted with a series of significant *challenges* when seeking out to regulate innovative technologies like cloud computing, ranging from conceptual to assessment problems, among other issues. The discussion of these challenges illustrates the need for enhanced and improved *interfaces* at the data, normative, and design levels of technology regulation.

---

[104] On an interop-based holistic approach to Internet regulation, *see* Ian Brown and Christopher T. Marsden, *Regulating Code: Good Governance and Better Regulation in the Information Age* (Cambridge: MIT Press, 2013).
[105] Gasser and O'Brien, "Governments and Cloud Computing."

It is in the zones of interface design and information exchange where cloud computing may ultimately – and perhaps in unexpected and currently underexplored ways – reflect back on the legal and regulatory system by enhancing its ability to better detect and more effectively respond to legal and regulatory issues in highly dynamic and complex technology environments.