nccr trade regulation
swiss national centre of competence in research

Working Paper No 2012/25 I JUNE 2012

Mapping Cloud Interoperability in the Globalized Economy: Theory and Observations from Practice

Urs Gasser and John Palfrey

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.

Mapping Cloud Interoperability in the Globalized Economy: Theory and Observations from Practice

URS GASSER AND JOHN PALFREY *
WITH MATTHEW BECKER

A. Introduction

Cloud computing describes an evolving paradigm in which many aspects of computing, including information processing, communication, networking, data acquisition, storage, and analysis, move from less efficient forms of localized production—for instance on a company's server or a user's laptop—to a system where a third party provides such resources and services on an aggregated, needs-based manner from remote locations.[1] To put it simply, 'the cloud' is a 'metaphor for externally or outsourced IT resources, information, software and hardware.'[2]

This article addresses the phenomenon of cloud computing in the globalized economy with a focus on one particularly important—and complex—policy issue: the question of *interoperability* in the cloud. Interoperability is the ability to transfer and render useful data and information across and among systems (including organizations), applications, or components, while also maintaining—if not enhancing—the core effectiveness of the services sharing the data.[3] The goal of this article is twofold. First, it seeks to introduce cloud interoperability as a topic with policy relevance against the backdrop of an emerging theory of interoperability.[4] Second and within this

* The authors wish to thank the participants of the Berkman Center for Internet & Society's 'Interoperability and the Cloud' Workshop (January 2011) for invaluable inputs and comments. Many thanks to Mira Burri for her collaboration and feedback, and to June Casey, Matthew Becker, Oliver Goodenough, Caroline Nolan, and the Berkman Center's interoperability team for research assistance and support. Special thanks to David O'Brien for collaboration.

[1] For an overview of cloud computing principles, *see* M. Armbrust, et al., 'Above the Clouds: A Berkeley View of Cloud Computing', University of California at Berkeley, Technical Report No. UCB/EECS-2009-28 (10 February 2009), available at: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf (last visited May 2012); P. Mell and T. Grance, 'The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology', NIST Special Publication 800-145, September 2011, p.2, available at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (last visited May 2012).

[2] L. Abad, 'Technology Forecast: Cloudy with a Chance of US Export Fines', *KPMG* (2011), p. 2, available at: http://www.us.kpmg.com/microsite/taxnewsflash/2011/Feb/Export_Issues_Cloud_Computing.pdf (last visited May 2012).

[3] U. Gasser and J. Palfrey, 'Breaking Down Digital Barriers: When and How ICT Interoperability Drives Innovation', Berkman Center Research Publication No.2007-8, 31 October 2007, available at: http://ssrn.com/abstract=1033226 (last visited May 2012).

[4] This article is an extension of the authors' larger text on interoperability—*Interop: The Promise and Perils of Highly Interconnected Systems*—in which they present a theory and framework for understanding the broader issues associated with interconnectedness in complex systems. U. Gasser and J. Palfrey, *Interop: The Promise and Perils of*

framework, it aims to highlight the interoperability issues that are implied and amplified within a cloud computing ecosystem. Through two real-world use cases, we will explore the practical challenges presented by these issues and outline a series of potential approaches to resolving them. In the process, we will also consider the role that various stakeholders, especially governments, can play in confronting them.

To set the stage, section B starts with a brief introduction to cloud computing, maps some of its key drivers, and provides a high-level overview of some benefits and key challenges.[5] We then put forth and describe a theoretical framework at the intersection of cloud technology, markets, and law: cloud interoperability. We argue that cloud interoperability is among the key challenges that deserve attention from cloud providers, intermediaries, users, and policymakers alike. After mapping the various dimensions of the interoperability challenge in the cloud in section C, we take a closer look, in section D, at select problems that emerge as witnessed in two real-world use cases where the various layers of interoperability come together and identify current approaches to these challenges. Section E offers our conclusion, outlining considerations regarding the different roles governments can play to support cloud interoperability across the different layers.

B. Move to the Cloud

I. Definition

Although cloud computing has become a familiar buzzword, it has been used in a variety of ways across diverse industries to describe a wide range of cloud-based technologies, services, and approaches. A uniform definition remains a work in progress. For the purposes of this paper, we rely on the definition of the US National Institute of Standards and Technology (NIST), which defines cloud computing as a 'model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing systems (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.'[6]

In addition to this definition, NIST lists the following five 'essential characteristics' that are helpful to gain a deeper understanding of the contours of the cloud phenomenon: (i) on-demand self-service, (ii) broad network access, (iii) resource pooling, (iv) rapid elasticity, and (v) measured service.[7]

From an interoperability perspective, even more important than the technical definition is the observation that cloud computing can be divided into three basic service models, as discussed in the next sub-section.

Highly Interconnected Systems (New York: Basic Books, 2012).

[5] This part of the paper is based on a research wiki on cloud computing law and policy issues created by the Berkman Center for Internet & Society's cloud computing research team. For access to the wiki, a list of publications, and resources associated with the Berkman Center's cloud computing research, *see* Berkman Center for Internet & Society, 'Cloud Computing Research', available at: http://cyber.law.harvard.edu/research/cloudcomputing (last visited May 2012).

[6] *See* P. Mell and T. Grance, above note 1.

[7] *Ibid.*, p.2.

II. Service and deployment models

NIST offers the following taxonomy of cloud service models.[8] The first is the cloud Software as a Service (SaaS), a model in which certain software applications are outsourced to a cloud provider that develops and maintains these applications on an underlying cloud infrastructure that includes network, servers, operating systems, and storage.[9] These and other components are controlled and maintained by the provider, while the cloud user can simply access the applications running on top of this infrastructure via various devices such as laptops, tablets, mobile phones, or the like and usually through thin client interfaces such as a standard web browser. This eliminates the need for users to install and run applications on their own computers; rather, they can simply access the necessary service via the Internet, thus simplifying maintenance and support. Examples of cloud SaaS include Gmail, Microsoft Online Services, and NetSuite.

A second service model is called Platform as a Service (PaaS).[10] As in the SaaS scenario, the cloud provider controls and operates a hardware infrastructure, such as the servers and network. and a basic software environment for executing applications, including an operating system. However, unlike the SaaS model, it is the cloud user who deploys the applications and may even control the respective application hosting configurations. In simple terms, the consumer 'rents' from the cloud provider the basic computing infrastructure to run consumer-created or consumer-acquired applications on top of it—which in turn are supported by the cloud platform provider. Examples include Microsoft's Azure and Google's App Engine.

Infrastructure as a Service (IaaS) is the third category of service model.[11] In this scenario, the capabilities provided by the cloud provider are processing, storage, networks, and other fundamental computing resources where the user is able to deploy and run software, including operating systems and applications. The cloud user does not manage or control the underlying cloud infrastructure, but has control over operating systems, storage, deployed applications, and eventually select networking components.[12] Amazon's Elastic Compute Cloud (Amazon EC2) is a familiar example; IBM, VMware, HP and other traditional IT vendors also offer IaaS services.

It is important to note that the service models outlined by the NIST taxonomy are not all-encompassing. They place a strong emphasis on the *means* for deploying applications; other categorizations focus more heavily on other *attributes* of cloud-based activities. For instance, some have suggested an alternative label—Data Storage as a Service (DaaS)—for services where data storage is the primary goal, such as Amazon's Cloud Drive.[13] It is also worth noting that individual business models may combine different dimensions of the taxonomy, supplying infrastructure, platform, software, storage, and connectivity as a combined service—consider in this light the offerings of consumer-facing cloud services, such as Google+, LinkedIn, or Facebook. Finally, different types of cloud deployment models exist. Private clouds, for instance, are only operated for one single organization. A public cloud, by contrast, is a computing

---

[8] F. Liu et al., 'NIST Cloud Computing Reference Architecture: Recommendations of the National Institute of Standards and Technology', NIST Special Publication 500-292, September 2011, pp. 20-21, available at: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505 (last visited May 2012).
[9] *Ibid.*, pp. 20-21.
[10] *Ibid.*, p. 21.
[11] *Ibid.*, p. 21.
[12] P. Mell and T. Grance, above note 1, p. 2.
[13] *See e.g.* Storage Networking Industry Association, 'Data storage as a Service (DaaS)', available at: http://www.snia.org/education/dictionary/d#data_storage_as_a_service (last visited May 2012).

infrastructure that is made available to the general public or multiple organizations. And there are several hybrid variations of these models as well.[14]

III. Drivers and benefits

Cloud computing comes with many advantages that drive its adoption across industry sectors.[15] For the private-sector organizations, the cost savings associated with cloud services are particularly important. When using cloud services, companies can avoid the massive upfront IT investments that would usually go into legacy servers and storage systems. Instead, they can deploy highly reliable, secure, and flexible (i.e. in terms of scalability) computing resources as needed and on a pay-per-use basis. Cloud computing can also eliminate the need to build costly IT departments, as the infrastructure is developed and maintained by the cloud-service provider. Such costs savings can be especially important for small and medium-sized enterprises.[16]

In addition to intra-organizational cost saving, recent surveys indicate that cloud computing can help organizations to recover from the current global economic downturn,[17] which can decrease transaction costs of IT-based services in cross-border business transactions.

Cloud computing comes also with benefits when looked at it from a macro level. By reducing IT costs, it can incubate and inspire innovation across the economy and enable a broad range of entrepreneurial activity, which can in turn strengthen the economy overall. Further, cloud computing is a driver of trade. Physical cloud technology is a tradable good itself. Even more importantly, cloud computing is the 'new global highway' that facilitates increasingly efficient and less costly forms of trade, as goods and information can be exchanged at a fraction of historical costs.[18] Against the backdrop of these economic drivers, the cloud-services market is expected to reach USD $127 billon by 2017, according to a recent report by Global Industry Analysts.[19]

But not only have companies embraced cloud services. Governments and individual consumers

---

[14] P. Mell and T. Grance, above note 1, p. 3.

[15] *See e.g.* Microsoft, 'The Economics of the Cloud', November 2010, available at: http://www.microsoft.com/en-us/news/presskits/cloud/docs/The-Economics-of-the-Cloud.pdf (last visited May 2012); M. Armbrust et al., above note 1; Federico Etro, 'The Economics of Cloud Computing', *The IUP Journal of Managerial Economics,* Vol. IX, No. 2 (May 2011), pp. 7-22, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2018109 (last visited May 2012).

[16] *See e.g.* J. McKendrick, 'Cloud computing employed at one-third of small and medium businesses: study', *ZDNet*, 9 August 2011, available at: http://www.zdnet.com/blog/service-oriented/cloud-computing-employed-at-one-third-of-small-and-medium-businesses-study/7431 (last visited May 2012); R. Ray, 'The Growing Cloud-Computing Market for SMBs', *Business Insider*, 18 July 2011, available at: http://articles.businessinsider.com/2011-07-18/tech/29981664_1_cloud-computing-cloud-services-smb-market (last visited May 2012).

[17] J. Burt, 'Sun CTO: Recession Fueling Interest in Cloud Computing, Virtualization', *eWeek*, 5 March 2009, available at: http://www.eweek.com/c/a/Virtualization/Sun-CTO-Recession-Fueling-Interest-in-Cloud-Computing-Virtualization (last visited May 2012); J. Scott, 'Has the recession accelerated cloud computing?', *ITPro*, 24 March 2010, available at: http://www.itpro.co.uk/621745/has-the-recession-accelerated-cloud-computing (last visited May 2012).

[18] 'The Global Economics of Cloud Computing', Cloud Computing World, available at: http://www.cloudcomputingworld.org/cloud-computing-for-businesses/the-global-economics-of-cloud-computing.html (last visited May 2012).

[19] Press Release,'Global Cloud Computing Services Market to Reach US$127 Billion by 2017, According to New Report by Global Industry Analysts, Inc.', *SFGate,* 21 November 2011, available at: http://www.sfgate.com/cgi-bin/article.cgi?f=/g/a/2011/11/21/prweb8977106.DTL&ao=all (last visited May 2012).

around the world are increasingly relying on cloud services. One of the most comprehensive government cloud strategies to date, for instance, has been developed and implemented by the US federal government. The model suggests that approximately USD $20 billion of the $80 billion spent by the US government on legacy IT services can be migrated to cloud computing solutions, potentially resulting in an estimated 30 percent savings in federal data center infrastructure costs.[20] Many other countries around the world—including the UK,[21] Japan,[22] Australia,[23] and, most recently Switzerland,[24] to name a few[25]—have also adopted government strategies to optimize efficiency, access, and functionality using cloud computing.

Individual consumers also rely on cloud computing infrastructure and services for ease-of-use and cheaper satisfaction of consumer needs.[26] Users of many e-commerce sites such as online travel agencies or web-based email services like Gmail, Yahoo! or Hotmail have been using cloud-based services long before 'cloud computing' became a household term. Starting with MySpace and now most prominently Facebook, social networking sites that allow the creation of online profiles and the sharing of content such as music, videos, news, etc. have been key drivers of everyday usage of cloud services by end users. Many of today's popular social media services—for instance, Twitter or YouTube—are, ultimately, cloud-based services.[27]

---

[20] V. Kundra, US Chief Information Officer, 'Federal Cloud Strategy', 8 February 2011, p.7, available at http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf (last visited May 2012).

[21] The UK government established G-Cloud, a private Government Cloud Computing Infrastructure, which includes IaaS, PaaS, and SaaS. For more information about the G-Cloud and UK governmental efforts in cloud infrastructure, *see* 'G-Cloud – Government Cloud Computing Program', *Cloudbook.net*, available at: http://www.cloudbook.net/directories/gov-clouds/gov-program.php?id=100018 (last visited May 2012).

[22] As part of the Digital Japan Creation Project (ICT Hatoyama Plan), Japan's Ministry of Internal Affairs and Communications revealed plans to create the 'Kasumigaseki Cloud' (tentative name) to be implemented by 2015. The Kasumigaseki Cloud is visioned to allow systems across numerous ministries to collaborate on the single cloud. For more information about the Kasumigaseki Cloud and the Digital Japan Creation Project, *see* 'MIC Communications News Vol.20 No.1 - MIC Announces the Outline of Digital Japan Creation Project (ICT Hatoyama Plan)', Ministry of Internal Affairs and Communications, available at: http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/NewsLetter/Vol20/Vol20_01/Vol20_01.html (last visited May 2012).

[23] In April 2011, the Australian Government Department of Finance and Deregulation released the Cloud Computing Strategic Direction Paper that stated that 'agencies may choose cloud-based services where they demonstrate value for money and adequate security'. Australian Government Department of Finance and Deregulation, 'Cloud Computing Strategic Direction Paper', Version 1, April 2011, available at: http://www.finance.gov.au/e-government/strategy-and-governance/docs/final_cloud_computing_strategy_version_1.pdf (last visited May 2012).

[24] Following a number of preliminary studies, in November 2011 the Swiss government published a strategy for implementing cloud computing services as part of its suite of e-government initiatives. For the publication (in German), *see* Informatikstrategieorgan, 'Cloud-Computing-Strategie der Schweizer Behörden', Schweizerische Eidegenossenschaft, 14 November 2011, available at: http://www.isb.admin.ch/themen/architektur/00183/01368/01372/index.html (last visited May 2012).

[25] *See e.g.* D. C. Wyld, 'Moving to the Cloud: An Introduction to Cloud Computing in Government', IBM Center for the Business of Government, 2009, pp.30-31, available at: http://www.etransform.org/gti/sites/etransform.org/files/Documents/2010-07%20IBM%20Business%20of%20Gov%20-%20Cloud%20Computing%20in%20Government.pdf (last visited May 2012).

[26] *See e.g.* S. Martin, 'Demystifying cloud computing for consumers', *USA Today*, 23 June 2011, available at: http://www.usatoday.com/tech/news/2011-06-22-cloud-consumer-apple-google_n.htm (last visited May 2012).

[27] 'Twitter and Cloud Computing', *Cloud Computing World*, available at: http://www.cloudcomputingworld.org/cloud-computing-for-businesses/twitter-and-cloud-computing.html (last visited May 2012).

Efficiency, access, and functionality are the most cited benefits of cloud services, and often act as the key drivers of cloud adoption across all sectors. But as discussed elsewhere in greater detail,[28] cloud computing has the potential to create value along a number of dimensions in addition to the classic gains of efficiency afforded by the centralization of production by offering opportunities for emergent values—products and services that come into existence as a result of the cloud itself.

IV. Challenges

The trend towards cloud computing comes with enormous economic benefits, creating new opportunities for collaboration, exchange, and large-scale experimentation. But it also comes with significant risks. From a *legal and policy perspective*, privacy is among the most pressing cloud issues.[29] The basic principles of cloud architecture—which often implicate third-parties, sets of geographically-diverse hardware infrastructure, and sensitive data processing and storage —highlight the need for a regulatory framework that addresses individual rights and related issues, such as data quality, processing transparency, and international transfers. Closely linked to privacy issues are concerns regarding data security, standards, international jurisdiction, contractual rules, and legal obligations.[30] Economic regulation, law enforcement considerations, and national security obligations are also pressing issues which require the development, implementation, and operation of retention practices in the cloud, which have to be balanced against other legitimate rights and civil liberties.

Several other concerns can be added to such data-related law and policy issues. Important cross-

---

[28] See Berkman Center for Internet & Society, above note 5.

[29] *See e.g.* P. Lanois, 'Privacy in the Age of the Cloud', *Journal of Internet Law*, vol. 15, no. 6 (December 2011), pp. 3-13; J. Soma, M. Nichols, M. Gates, A. Gutiérrez, 'Chasing Clouds Without Getting Drenched: A call for fair practices in cloud computing services', *Journal of Technology Law and Policy*, 16 (December 2011), pp. 193-227; D. M. Parrilli, 'Legal Issues in Grid and Cloud Computing' in K. Stanoevska-Slabeva, T. Wozniak, and S. Ristol (eds.), *Grid and Cloud Computing: A Business Perspective on Technology and Applications* (Berlin: Springer, 2010), pp. 97-118; M. Armbrust et al., 'A View of Cloud Computing', *Communications of the ACM*, vol. 53, no. 450 (2010), p. 50, available at: http://www.csee.usf.edu/~anda/CIS6930-S11/papers/cloud-computing-armbrust.pdf (last visited May 2012); R. L. Grossman, 'The Case for Cloud Computing', 11 *IT Professional* 25-27,11, 2 (March-April 2009), pp. 25-27, available at: http://www.cmlab.csie.ntu.edu.tw/~freetempo/CN2011/hw/hw1/04804045.pdf (last visited May 2012); N. Leavitt, 'Is Cloud Computing Really Ready for Prime Time?', IEEE – *Computer* (January 2009), pp. 18-20, available at: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4755149 (last visited May 2012); R. Gellman, 'Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing', World Privacy Forum, 23 February 2009, available at: http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf (last visited May 2012); Siani Pearson, 'Taking Account of Privacy when Designing Cloud Computing Services', *HP Laboratories*, HPL-2009-54, 6 March 2009, available at: http://www.gtsi.com/eblast/corporate/cn/09_09_2009/PDFs/HP%20Lab.pdf (last visited May 2012).

[30] One of the pressing examples with regard to privacy and jurisdiction deals with the conflict between the USA PATRIOT Act and the European Union's Data Protection Directive, as the PATRIOT Act may allow the data being stored or used in US-based cloud computing services to be disclosed to the US authorities without prior consent from, or notice to, the user. *See* discussion on legal and policy interoperability, below notes 66, 80 and accompanying text; *see also* J. Baker, 'EU Upset by Microsoft Warning About US Access to EU Cloud', *PCWorld*, 5 July 2011, available at: http://www.pcworld.com/article/235041/eu_upset_by_microsoft_warning_about_us_access_to_eu_cloud.html (last visited May 2012); J. Stokes, 'PATRIOT Act Gives Foreigners Good Reason to Avoid US Clouds', *Wired Cloudline*, December 2011, available at: http://www.wired.com/cloudline/2011/12/us-cloud (last visited May 2012).

sectional issues, including transparency, responsibility, and clarity must characterize the contractual and regulatory frameworks that govern cloud computing, and the complex technological, organizational, and economic settings such in which it occurs. Linked to transparency and a key element for providing appropriate safeguards is the clarification of legal and ethical responsibilities of the diverse range of stakeholders who operate within the cloud ecosystem. Approaches to be considered in this context range from more traditional instruments of criminal law, civil liability, and risk insurance to concepts such as corporate social responsibility.

Additional legal and policy issues that are of great importance in the cloud environment include the question of jurisdiction—including the international application laws and enforcement authority—as data increasingly flows across borders of nation states.[31] More recently, the legal and ethical obligations (or the lack thereof) of private-sector cloud companies that control speech in the digitally networked public sphere has come up for discussion. A trend towards market concentration, triggered by the enormous costs of building data centers as core infrastructure elements of deeper layered cloud service models, is another policy concern that has emerged and needs to be addressed in the context of competition law.

Some of these problems are already well known challenges in the Internet age, others are different in scale or new in kind. Perhaps the most complex challenge at the intersection of technology, markets, and law, however, is the issue of cloud interoperability[32] and portability.[33] As noted in the introduction, we define interoperability as the ability to transfer and render useful data and other information across systems (including organizations), applications, or components. Applied to the cloud environment and at the most basic level, interoperability enables a cloud

---

[31] *See e.g.* D. Harris, 'Tech Giants to Feds: We need free trade for data', *GigaOm*, 4 November 2011, available at: http://gigaom.com/cloud/tech-giants-to-feds-we-need-global-free-trade-for-data (last visited May 2012); C. Kuner, 'Data Protection Law and International Jurisdiction on the Internet (Part 1)', *International Journal of Law and Information Technology,* 18, 2 (2010) pp. 176-193, available at: http://ijlit.oxfordjournals.org/content/18/2/176.extract (last visited May 2012); V. Narayanan (student comment), 'Harnessing the Cloud: International Law Implications of Cloud-Computing', *Chicago Journal of International Law*, vol. 12 (Winter 2012), pp. 783-809; A. Thierer and W. Crews (eds.) *Who Rules the Net?* (Washington, D.C.: Cato Institute, 2003). There have been a number of cases directly related to these issues. *See e.g.* Information and Privacy Commissioner for British Columbia, 'Privacy and the USA PATRIOT Act: Implications for British Columbia Public Sector Outsourcing', October 2004, available at: http://www.steptoe.com/assets/attachments/400.pdf (last visited May 2012); Clark Wilson LLP, 'British Columbia's Privacy Laws Amended In Response to the USA PATRIOT Act', available at: http://www.cwilson.com/services/18-resource-centre/190-british-columbias-privacy-laws-amended-in-response-to-the-usa-patriot-act.html (last visited May 2012); Jan-Jaap Oerlemans, 'Belgium vs Yahoo!', *OerlemansBlog*, 3 February 2011, available at: http://oerlemansblog.weblog.leidenuniv.nl/2011/02/03/belgium-vs-yahoo (last visited May 2012) .

[32] A large number of companies supported the 'Cloud Manifesto' in 2009, agreeing to cloud computing interoperability. Most recently, a couple of large technology companies including IBM, Cisco, EMC, CA, SAP, and Red Hat agreed to a standard for cloud portability. Topology and Orchestration Specification for Cloud Applications (TOSCA) aims for increased service and application portability. For more information on the cloud manifesto, *see* 'Open Cloud Manifesto.org', available at: http://www.opencloudmanifesto.org (last visited May 2012). For more information on the TOSCA *see* http://tosca-open.org (last visited May 2012); T. Samson, 'Tech giants back standard cloud portability', *Infoworld*, 16 January 2012, available at: http://www.infoworld.com/t/cloud-computing/tech-giants-back-standard-cloud-portability-184160 (last visited May 2012).

[33] *See e.g.* A. L. Diaz, 'Develop a cloud adoption strategy to maximize ROI for new or existing services', *WIRED Cloudline*, September 2011, available at: http://www.wired.com/cloudline/2011/09/if-it-is-not-interoperable-if-it-is-not-portable-it-is-not-cloud (last visited May 2012).

user to move her data into the cloud and out—or more precisely, to work with one cloud-service provider and retain the ability to transfer the data from this service to another, preventing a situation of lock-in.

C. Mapping Cloud Interoperability: Four Conceptual Lenses

I. Layers of interoperability

A growing body of scholarship that studies interoperability problems in the digital environment points out that interoperability is typically multi-dimensional.[34] Although no uniform taxonomy exists, the organization of these different dimensions in the form of a four-layered 'cake model' has proven helpful when analyzing and assessing interoperability problems from a law and policy perspective:[35]

- *Technical interoperability*: Interoperability at the technological layer means in the most basic sense that systems—such as the hardware and the code in computing systems or the train track in the transportation system—can connect to one another, often through an agreed-upon interface.
- *Data interoperability*: The data layer is closely linked to the technology layer, but adds another dimension to it. It is not enough that systems can exchange signals. The signals and data that are passed across systems, applications, or components must be 'understandable' to the receiving entity. Sometimes, this layer is also called 'semantic' interoperability.
- *Human interoperability*: This describes the ability of humans at either side of the exchange of data to understand what the other person is saying and to act upon that exchange. Language or a shared vocabulary is one manifestation of human interoperability. Cultural issues are also embedded in the human layer, and can play a powerful role in the success or failure of an otherwise interoperable system.
- *Institutional interoperability*: Analogous to the human context, institutional interoperability describes the meaningful working together among institutions. As sets of rules with corresponding enforcement mechanisms, institutions include not only organizations, but legal institutions and policy systems as well.

Typically, we understand the relevance and meaning of the different levels of interoperability in a given technological context the clearest when looking at a practical example. Consider, for instance, a system of electronic health records that is operated in a cloud environment.[36] E-health records require that computers, software, and various other technical systems are able to

---

[34] Gasser and Palfrey, 'ICT Interoperability', above note 3; *see also* Stacy A. Baird, 'Government Role and the Interoperability Ecosystem', *Journal of Law and Policy for the Information Society* vol. 5, no. 2 (Summer 2009), pp. 219-290, available at: http://ssrn.com/abstract=1482752 (last visited May 2012).

[35] Gasser and Palfrey, *Interop*, above note 4, pp. 5-7, Chatper 1: 'The Technically and Data Layers', pp. 21-37, Chapter 2: 'The Human and Institutional Layers', pp. 39-53.

[36] U. Gasser and J. Palfrey, 'Fostering innovation and trade in the global information society: The different facets and roles of interoperability' in M. Burri and T. Cottier (eds.), *Trade Governance in the Digital Age* (Cambridge: Cambridge University Press, 2012).

exchange useful data with one another (technical interoperability). In addition, the workflows of physicians, laboratories, hospitals, insurance companies, and other organizations need to be interoperable (data interoperability). Further, these exchanges of information and the synchronization of workflows need to be backed-up by organizational and legal safeguards to ensure security and privacy, among other things (institutional interoperability). Finally, the people involved across institutions need to have the necessary degrees of digital literacy (and share a particular culture of collaboration) in order to harness the full benefits provided by electronic health records (human interoperability).[37]

II. Vertical and horizontal interoperability[38]

In addition to the 'layered cake' model described above in sub-section I, cloud computing interoperability can be usefully conceptualized along two dimensions—vertical and horizontal. The vertical dimension describes how cloud computing facilitates interoperability within a single platform, such as between different devices and applications utilized by the same consumer or end-user. When someone uses Gmail, for example, it is possible to access one's email messages from any Internet connected computer, including smartphones. In contrast, the horizontal dimension describes interoperability across platforms, such as moving from one cloud platform another service available at lower-cost or under better terms.

1. Vertical Dimension

The vertical dimension concerns interoperability within the cloud, generally from an end-user or consumer's perspective: does the cloud-based software work on most Internet-enabled devices? Can it make use of other applications or data that are accessible from the user's devices?

The vertical dimension is important because it facilitates both *device independence* and *location independence*, two elements that are intrinsically bound. When a user accesses her data or services from the cloud, she is no longer constrained to the single computer that would otherwise store the data or run the application—generally, any device with an Internet connection will often suffice. Because processing and storage may be performed in the cloud, she can use programs or access information on light, relatively low-performance *thin clients* (e.g. computers or programs that rely on network-connected servers for most of their processing needs), such as netbooks and smartphones. Similarly, both factors contribute to location independence: the ability to access data and applications anywhere with any Internet-connected device, regardless of its location. Such remote processing and storage capabilities might prove to be especially useful in developing nations, where access to technological infrastructure may be limited.[39]

2. Horizontal Dimension

The horizontal dimension concerns interoperability between competing cloud computing

---

[37] M. J. Ball and J. Lillis, 'E-health: transforming the physician/patient relationship', *International Journal of Medical Informatics*, vol. 61, no. 1 (April 2001), pp.1-10, pp.1-2.

[38] For a detailed discussion, see M. B. Becker, 'Interoperability Case Study: Cloud Computing', Berkman Center Research Publication No.2012-11, 28 April 2012, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2046987 (last visited May 2012).

[39] M. R. Nelson, 'Briefing Paper for the ICCP Technology Foresight Forum – Cloud Computing and Public Policy', Organisation for Economic Co-operation and Development (OECD), document no. DSTI/ICCP(2009)17, 14 October 2009, p.4, available at: http://www.oecd.org/dataoecd/39/47/43933771.pdf (last visited May 2012).

services: how easily can a business that has its software hosted in one cloud service move to a competing cloud provider who offers more favorable rates or more reliable service? Are there consistent means of coordinating between cloud products, such as standardized contractual arrangements, security features, data privacy, or means of identity management (both for authentication and attribution)? The horizontal dimension can relate both to consumers and the companies that purchase cloud products.

The horizontal dimension exhibits a common problem among interoperable technologies: 'lock-in', or what is sometimes called 'stickiness'.[40] Because it is not always easy to port data or applications from one cloud service to another, it is possible for users of cloud services—whether they are businesses, organizations, or end-users/consumers—to get 'locked in' to using a particular cloud service. In this scenario, horizontal interoperability faces a primary problem where cloud providers do not have much of an incentive to make their services interoperable because it would then only make it easy for users to pick up their data and leave for another cloud.

The horizontal dimension includes not only technical barriers for moving between cloud products and services, but also incompatibilities or inconsistencies between data privacy and security policies, identity management, and standard contractual arrangements—such as 'terms of service' and 'service-level' agreements—with regards to different cloud providers. Any such inconsistency may hinder movement between providers, and it may also limit a business or an organization's ability to draw on the resources of multiple providers. For instance, a hospital operating under strict confidentiality laws would need its cloud service providers to also implement strong privacy rules and security standards.[41] Although these standards need not be identical, the greater the uniformity between them, the easier it will be for the hospital to evaluate potential liabilities.

III. Interoperability, portability, and cloud-service models

Another important finding resulting from interoperability policy research is the observation that interoperability is highly context-specific. It means different things to different stakeholders in different contexts.[42] Consequently, when approaching interoperability as a policy issue, it is particularly important to take into account the specific technological, economic, legal, and social parameters of a given environment in which the issue arises. Applied to cloud computing, it is therefore necessary to be specific about the particular service model in question. The technological layer is illustrative in this respect and demonstrates how the issues might change when considering different services models and when moving from one sub-context to another.

As mentioned above in Section B, the cloud computing service models can be roughly distinguished as: SaaS, PaaS, and IaaS. The technological interoperability issues are quite distinct for each model (similar differences could be identified when looking at it from an economics perspective, for example).

---

[40] *See* R. Picker, 'Competition and Privacy in Web 2.0 and the Cloud', *Northwestern University Law Review Colloquy*, vol. 103 (July 2008), pp. 1-12; S. Liebowitz and S. Margolis, 'Path Dependence, Lock-in, and History', *Journal of Law, Economics, & Organization*, vol. 11 (April 1995), pp. 205-226.

[41] *See* P. Kominers, 'Interoperability Case Study: The Internet of Things', Berkman Center Research Publication No.2012-10, 1 April 2012, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2046984 (last visited May 2012).*see also* Berkman Center for Internet & Society, above note 5.

[42] Gasser and Palfrey, 'ICT Interoperability', above note 3.

A 2011 NIST report on cloud computing standards, which maps the different standards for interoperability, illustrates the level of complexity.[43] The report looks at the different types of cloud interfaces and distinguishes between two major categories: *functional interfaces* (to what is resident in the cloud) and *management interfaces* (through which cloud users manage their use of the cloud); both have interoperability needs that need to be determined and approached separately.[44] Moreover, the interoperability issues that characterize each category vary across the three service models. To give an example: in the case of SaaS, the functional interface is the same as the application interface of the software itself. In cases where the application is consumed through a Web browser, existing and non-cloud-specific standards are used to achieve interoperability. By contrast, the functional interface in the IaaS model is often tied to the processor architecture (i.e. CPU) and other input/output hardware components that are being virtualized and not a candidate for standardization.[45] At the same time, the self-service IaaS management interface is subject to standardization as a means to increase interoperability. In contrast to the SaaS example, these efforts must be cloud specific (e.g. Open Cloud Computing Interface; Cloud Data Management Interface standard, etc.).[46]

These few examples suggest the importance of context-specificity when it comes to cloud interoperability analysis. They also demonstrate the need for interdisciplinary approaches when analyzing and addressing interoperability problems in the cloud, especially when looking at concrete use cases where different layers of interoperability play together and further complicate the analysis, as we will discuss in the next section.

A particularly important subset of cloud computing interoperability concerns portability in the cloud. Broadly speaking, there are at least two different types of portability. First, there is a need for portability of certain elements of (virtual) cloud infrastructure across various cloud platforms. The Open Virtualization Format (OVF) is a standard that addresses, for instance, the portability between various virtualization platforms.[47] Second, storage and data portability is another critical dimension of portability in the cloud environment. Many users are concerned about their capacity to move their data between and within cloud environments. However, data portability is an issue where technical possibilities—leveraging existing data formats such as Extensible Markup Language (XML)—are not always aligned with business incentives, which may speak against higher levels of interoperability from a cloud service provider's perspective depending on its market position.

---

[43] M. Hogan, F. Liu, A. Sokol, and J. Tong, 'NIST Cloud Computing Standards Roadmap', NIST Special Publication 500-291, July 2011, available at: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909024 (last visited May 2012).

[44] *Ibid.*, p. 33.

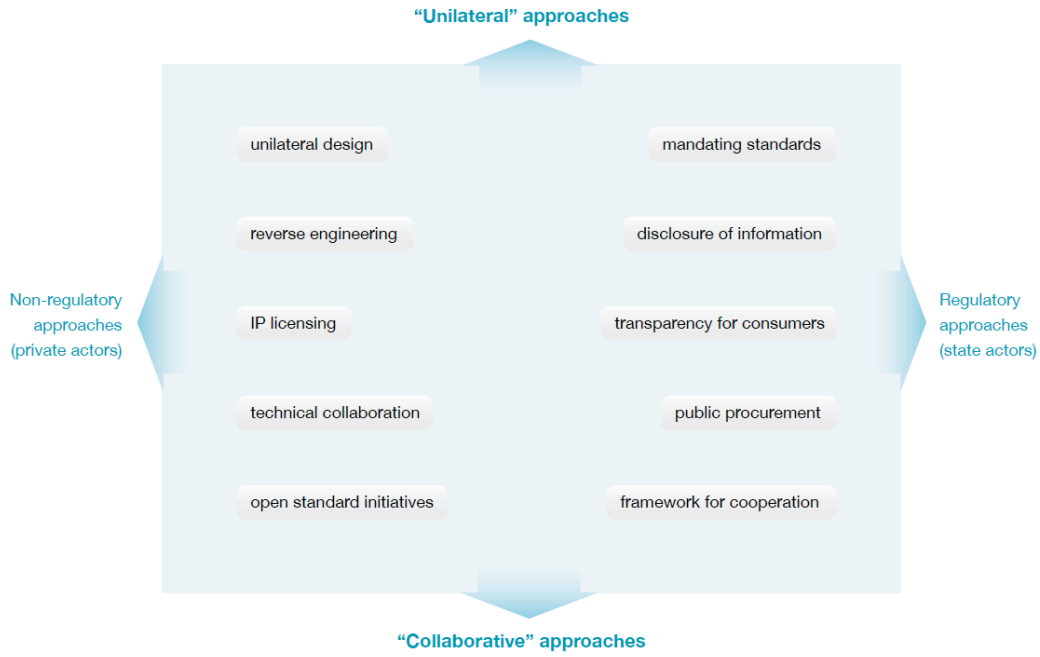
[45] Virtualization enables multiple computing environments to operate in parallel on a single CPU, to varying degrees, by using software, and to a lesser degree embedded functionality in hardware, to simulate specific hardware configurations. *See e.g.* VMware, 'Virtualization', http://www.vmware.com/virtualization (last visited May 2012).

[46] *Ibid.*, p. 34.

[47] *See* Distributed Management Task Force, Inc.,'Open Virtualization Format', http://www.dmtf.org/standards/ovf (last visited May 2012); Distributed Management Task Force, Inc., 'Open Virtualization Format Specification – version 1.1.0', document no. DSP0243, January 2010, available at: http://dmtf.org/sites/default/files/standards/documents/DSP0243_1.1.0.pdf (last visited May 2012); *see also* discussion on cloud standards-development organizations, below section D, III.

IV. Approaches to cloud interoperability

The emerging theory of interoperability in the digital age suggests that there are different tools available that can be used to work towards higher levels of interconnectedness among systems, components, and applications, particularly at the technical and data layers. The following chart provides an overview of general approaches, which can be roughly divided into unilateral versus collaborative approaches on the one hand and private versus government-based approaches on the other hand.[48]



Early indicators suggest that several of these approaches are likely to play an important role in the context of cloud computing interoperability. On the side of non-regulatory approaches, we have already mentioned the importance of standard-setting initiatives with regard to the specific issues of management interface interoperability as well as with respect to data formats. IP licensing and technical collaboration are other important interoperability-enabling strategies used by cloud providers, especially in the context of SaaS.

On the side of approaches driven by state actors, public procurement power has already been exercised as a tool to motivate cloud providers to increase certain aspects of cloud interoperability.[49] Governments can also serve as conveners to enable frameworks for cooperation among cloud providers with the goal of increasing interoperability. In the US, the NIST initiatives mentioned in the previous section are a great example of this approach.

Looking at the trajectories of other types of information and communication technologies, it is reasonable to expect that additional tools from the government's toolbox will be activated to

---

[48] Gasser and Palfrey, 'ICT Interoperability', above note 3, p. 20; *Interop*, above note 4, p. 15.

[49] Nelson, 'Cloud Computing and Public Policy', above note 39; *see also* M. R. Nelson, 'The Cloud, the Crowd, and Public Policy', *Issues in Science and Technology*, Summer 2009, pp. 71-76, available at: http://cct.georgetown.edu/Nelson%20Cloud%20Article.pdf (last visited May 2012).

address emerging interoperability issues—including, for instance, transparency requirements.

D. Selected Cloud Interoperability Issues and Approaches: Observations from Practice

I. Use cases

Given its context-specificity, central issues regarding interoperability and cloud computing are best understood through the challenges presented by real-world examples and cases in practice. Such examples can also be mined for additional insights regarding potential solutions or intervention points, even beyond the approaches outlined in the previous section.

The following two uses cases were used in the context of an interdisciplinary exploratory workshop convened by the authors and including diverse experts from academia, government, and industry.[50] Participants collectively identified and discussed key interoperability issues across the layers mapped above in section C, and considered the potential impact and limitations of different interventions and approaches. The first use case centers on person-to-person communications and the security and portability of data stored in a public cloud-hosted service or platform. The second use case builds upon the example noted earlier[51] and focuses on interoperability and portability issues related to cloud-based Electronic Medical Records (EMRs).

1. Use case A: Person-to-Person Cloud-hosted Communications

In reality, few users will 'use the cloud' directly. Rather, their interactions with different cloud services, like webmail, Facebook, IM, and Twitter, may result in their data or person-to-person communications being stored in some form in a service that uses cloud technology. Essentially, this information resides with the service provider or platform where it leaves a data trail. This raises questions and issues that need to be addressed: What standards should govern the portability of data objects and other information inside applications? How much do/should end-users 'own' their data across different cloud-based platforms and service providers? What is the role for industry, especially cloud service providers, in supporting different forms of interoperability at the technical, legal, and policy levels? For governmental actors, what questions arise from the movement and portability of data across borders?

2. Use case B: Electronic Medical Records (EMRs)

Policymakers around the world are grappling with opportunities and challenges portended by new technologies and their application to healthcare. The US provides a compelling case in point. US policymakers recognize the huge costs and inefficiencies at work within the sprawling US healthcare industry, which a 2005 RAND study deemed the world's largest and most inefficient information enterprise.[52] Despite the benefits, which include cost savings, quality enhancements, better care, and more efficient patient access, the potential costs are very real—large upfront

---

[50] *See* Berkman Center for Internet & Society, 'Workshop Report: Interoperability in the Cloud', January 2011, available at: http://cyber.law.harvard.edu/research/cloudcomputing (last visited May 2012).

[51] *See* discussion on electronic healthcare records, above section C, I.

[52] R. Hillestad, J. Bigelow, et al., 'Can Electronic Medical Healthcare Record Systems Transform Health Care? Potential Health Benefits, Savings, and Costs', *Health Affairs*, vol. 25, no. 5 (September 2005), pp. 1103-1117, 1103, available at: http://content.healthaffairs.org/content/24/5/1103.full (last visited May 2012).

capital investments, increased privacy and security risks, and the challenges of coordinating a hugely complex system. Although EMR systems have existed for more than thirty years, a relatively small number of hospitals and medical offices have fully-integrated EMR systems. A growing number of EMR system providers are beginning to roll out EMR systems across the country, but in individualized install bases. A number of technically distinct system architectures are being used throughout this process—the majority of which consist of proprietary storage formats which are not interoperable.

Considering the potential benefits that a nationally, or internationally, coordinated EMR system would provide, a number of interoperability questions arise from the technical, legal, policy angles: How will the systems work together? How will standards be developed and enforced, especially with regard to data storage, retention, and portability? What are the incentives for major actors, including the government and private companies, to work together to make EMRs possible? Interoperability can be foundational to efforts at the center of making a system of EMRs truly effective, but can itself be a barrier to its implementation.

II. Select practical issues emerging from use cases

These use cases provide an opportunity to evaluate the different layers and facets of the interoperability phenomenon as it relates to cloud computing from a *practical perspective*, which complements the theoretical perspective of the first half of this paper. It surfaces questions related to the roles and obligations of the different stakeholders within the cloud ecosystem—users, industry, platform providers and governments—and pushes us to consider some of the means (such as standards setting, transparency, and other tools) through which, when applied at appropriate levels, interoperability can be achieved. More specifically, an analysis of the two use cases reveals the following set of challenging interoperability issues at the intersection of technology, economics, law, and policy, and makes visible the links between these issues and related cloud policy matters, including privacy, security, and transparency, among others.

1. Technical interoperability and the portability of data

Data interoperability in the cloud is closely related to the topic of ownership of data,[53] which is relevant in both use cases, and intersects with policy, legal, and data interoperability. In the context of the first use case, service agreements[54] can play a role in setting parameters for how an end-user might interact with a cloud service and how that user's data ownership rights are governed. However, such agreements may result in the temporary (or permanent) transfer of certain data rights to the service provider by the end-user in exchange for using the cloud services.[55] From the cloud-service provider's perspective, 'data ownership' is not a single, easily portable right that accompanies an end-user's data to its next location. The lack of policy-based

---

[53] *See* M. Turilli and L. Floridi, 'Cloud Computing and its Ethical Challenges', paper presented at CEPE 2011: Crossing Boundaries, Milwaukee, Wisconsin, May 31 - June 3, 2011, pp. 280-284, abstract available at: http://users.gw.utwente.nl/Coeckelbergh/site/publicaties/Conference%20Proceedings.pdf (last visited May 2012).

[54] For consumers, these agreements are often referred to as 'Terms of Use' or 'Terms of Service' agreements; for large 'enterprise' organizations, these are oftened reffered to as 'service-level' agreements. *See e.g.* S. Bradshaw, C. Millard, and I. Walden, 'Contracts for Clouds: Comparison and analysis of the terms and conditions of cloud computing services', *International Journal of Law and Information Technology*, vol. 19 (Autumn 2011), pp. 187-223.

[55] In many cases, the exchange of certain data is valuable to the public-cloud service provider.

or legal interoperability between such agreements can weaken the ownership rights of users as they seek to move their data into or between clouds.

Even if ownership rights are clear or service-level agreements set the stage for high levels of interoperability, such arrangements will not solve data portability issues at the technical and data layers. That is, even if end-users have the legal right to port their data from one cloud service to another, the data must be packaged in such a way that it can be easily moved between those systems. Differences in application data formats (and to a lesser extent unique data organizations within cloud computing environments) may undercut this type of interoperability. A 'closed' data format[56] which is used by one cloud but may not be available for license or to be technically supported by another cloud service, can lock data into specific cloud platforms and render transfer between competing cloud providers costly or impossible. Similarly, two applications that use varying undocumented open formats may also be unable to communicate.

Although the use of a particular data format is to some extent guided by the type of cloud service being offered, formats can still differ greatly between similarly positioned cloud-service providers. A number of developmental considerations may drive cloud service providers to choose one format over another. For example, certain formats are better suited for certain tasks and, in cases where a cloud service provider offers a service with a unique capability, the service typically uses a unique format. At first, unique proprietary formats may appear to be inherently non-portable, but, after reaching a point of maturity in the market, the same formats may evolve into a *de facto* standard of choice for competitors.

However, it is important to note that cloud providers sometimes select proprietary formats *because* they lack portability. Service providers may perceive this lack of technical and/or data interoperability to be a competitive advantage, which they may endeavor to protect by keeping formats closed.[57] In this context, the proprietary data creates a barrier for end-users to transfer their data to a competitor's cloud and hinders their ability to migrate to other platforms. This type of competitive advantage is not limited to technical means, such as using non-portable data formats, since analogous lock-in effects can also be accomplished, to varying degrees, through service agreements.[58] A company that operates with significant network effects—consider the provider of social networking services, for example, as in the first use case—may have a strong incentive to lock-in its users by establishing such barriers that prevent horizontal interoperability among similar cloud services.[59]

---

[56] In contrast to an open format, which is usually maintained by a standards organization or publicly documented, a closed proprietary data format is not maintained by a standards organization, well-documented, or within the public domain and available for public use. Depending on the circumstances, the circumvention of closed proprietary formats may violate certain intellectual property rights (e.g. anti-circumvention provisions of the Copyright Act and exclusive rights granted to patent holders). *See e.g.* A. Peraznowski, 'Rethinking Anticircumvention's Interoperability Policy', *U.C. Davis Law Review* vol.42 (June 2009), pp. 1549-1620; M. Lemley, 'Intellectual Property Rights and Standard-setting Organizations', *California Law Review* vol. 90, (December 2002), pp. 1889-1973.

[57] Palfrey and Gasser, *Interop*, above note 4, Chapter 5: 'Competition and Uniformity', pp. 89-109.

[58] Some cloud service providers utilize 'data hostage provisions' which severely limit or prohibit an end-user's ability to fully terminate the agreement, transfer, or extract data. For example, some service providers require encumber the return of end-user data through 'right-to-cure' and liquidated damages provisions, and as well as arbitration clauses. *See* R. H. Carpenter Jr., 'Walking from Cloud-to-Cloud: The Portability Issue in Cloud Computing', *Washington Journal of Law, Technology & Arts* vol. 6, no. 1 (Summer 2010), pp. 1-14.

[59] Palfrey and Gasser, *Interop*, above note 4, Chapter 5: 'Competition and Uniformity', pp. 89-109.

Portability constraints are also raised in the health context, especially with regard to the use of different data formats by EMR-system providers.[60] One way to deal with this problem is to encourage EMR-system providers to digitize records as fast as possible (regardless of format) in order to move them to the cloud, and solve the issue of differing formats as the process evolves. Another approach is for industry players to make baseline decisions regarding technical and other standards first (most likely with government intervention), convert all the records into a standardized format and then put them into the cloud. The latter scenario will likely be inefficient due to the length of the policy development process; however, the lack of immediate interoperability in the former will also have disadvantages.

The advantages of embedding multi-layered vertical interoperability and portability of data is also evident in another informative example from the healthcare context: the collaborative use of Microsoft's HealthVault by patients and health care providers to manage diseases like diabetes and heart disease.[61] Patients at the Cleveland Clinic use at-home monitoring devices to measure glucose levels or heart rates, and upload their data to HealthVault. This data is then immediately available to the patients' health care providers at the Cleveland Clinic, allowing them to follow the patients' progress remotely and draw on more comprehensive and accurate data when meeting with the patient at the clinic.[62] Thus, HealthVault overcomes geographic boundaries through an impressive use of vertical interoperability, linking disparate individuals and machines: data is uploaded from a medical device via an internet-connected computer to a centralized repository, accessible by doctors at the Cleveland Clinic. This technology, referred to by some in the health tech and participatory medicine arena as a 'data utility layer', combines the data from multiple sources that would otherwise be incompatible (such as medical records, heart rate monitors, and pedometers) into a single source that can be accessed by the patient or the physician.[63] Similar technology has been well received by patients, and is believed to hold much promise for medical treatment.[64]

2. Legal and policy interoperability

In the globalized digital economy, data can transfer across national borders over a network connection with relatively few physical impediments. Jurisdictional complexities, on the other hand, present significant risks for cloud service providers and end-users. Each nation potentially

---

[60] D. J. Brailer, 'Interoperability: The Key To The Future Health Care System', *Health Affairs*, January 2005, available at: http://mendocinohre.org/rhic/jan2006/hlthaff.w5.19v1.pdf (last visited May 2012).

[61] Microsoft, 'Microsoft Health Vault', available at: http://www.microsoft.com/en-us/healthvault (last visited May 2012).

[62] F. Humphries, 'Congress Considers Cloud Computing', *TechNet Blogs: Microsoft on the Issues*, 22 September 2010, available at: http://blogs.technet.com/b/microsoft_on_the_issues/archive/2010/09/22/congress-considers-cloud-computing.aspx (last visited May 2012).

[63] M. Holt, 'Why We Need and Independent Health Data Utility', *The Health Care Blog*, 27 June 2011, available at: http://thehealthcareblog.com/blog/2011/06/27/why-we-need-an-independent-health-data-utility (last visited May 2012); G. Thompson, 'Health 2.0 Europe: A Personal Health Record (PHR) by Another Name…', *CLOUD Inc.*, 7 April 2010, available at: http://cloudinc.org/ecosystems/article/health-2-0-europe-a-personal-health-record-phr-by-another-name (last visited May 2012). Google Health was another example of a data utility layer in the health field, but the project was terminated by Google at the end of June 2011. *See* D. Linton, 'RIP Google Health', *Health 2.0 News*, 24 June 2011, available at: http://www.health2news.com/2011/06/24/rip-google-health (last visited May 2012).

[64] A. Watson et al., 'Diabetes Connected Health: A Pilot Study of Patient- and Provider-Shared Glucose Monitoring Web Application', *Journal of Diabetes Science and Technology*, vol. 3, no. 2 (March 2009), pp. 345-352, available at: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2771507 (last visited May 2012).

has opposing substantive notions and legal requirements, in addition to conceptions and standards related to privacy and security. End-users from different nations may also have distinct expectations of privacy and security. These differences can hinder the progress of global interoperability, particularly with regard to cross-border data flow, storage, and portability.

For cloud-service providers, 'data sovereignty' poses the most significant legal considerations and risks—that is, is the data subject to the jurisdiction where it is physically stored or hosted on servers?[65] Local laws may permit the government, or its law enforcement agencies, to easily compel disclosure of sensitive data. For example, under the USA PATRIOT Act law enforcement agencies are capable of gaining access to personal financial information, e-mail, and any other forms of electronic communications after merely certifying that the information sought is relevant to an ongoing criminal investigation.[66] Enterprise end-users of cloud services are especially aware of the cross-jurisdictional data disclosure risks, and, consequently, are hesitant to use those cross-border services unless the cloud service provider stipulates that they will only store the data within a particular jurisdiction. However, it is worth noting that higher expectations and substantive regulations in some jurisdictions may be unattractive to service providers in terms of costs associated with regulatory compliance and can therefore impede cross-border flows.

In contrast to enterprises using cloud services, consumer end-users face a slightly different set of risks: security breaches and disclosure of personally identifiable or otherwise private information. Public cloud service providers possess—and sometimes own[67]—a wide range of sensitive end-user data; consider, for example the first use case examples related to troves of data related to person to person communications. Depending on the type of cloud service at issue, this can include financial information, contents of emails, biographical information, medical history, and other categories of information that, if compromised, can be used to perpetuate identity fraud. Each jurisdiction may potentially treat these categories of information differently. Such jurisdictional complexities are amplified even further in the context of the second use case. The idea of EMR systems that have global reach or capacity would raise many data privacy, security, and portability concerns. Even though such a system would have enormous value, the highly sensitive and multi-jurisdictional aspects of globalized EMRs would require broad consensus in technology and policy.

III. Practical approaches to increase interoperability in the cloud

1. Technical interoperability and the portability of data

As noted in the previous section, a key barrier to data portability between companies and countries is the lack of open and standardized infrastructure formats for data. Technical standardization—one of the instruments available to increase interoperability—could be one way

---

[65] Although the location of where the data is stored or hosted is a primary factor in determining jurisdictional reach, it is not by itself dispositive. Inter-jurisdictional ambiguity remains a problem in areas where local laws or regulations attempt to regulate transient data. *See also* Kuner, 'Data Protection Law', above note 31.

[66] 'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism' (USA PATRIOT) Act of 2001', Public Law No 107-56, 115 Stat. 272 (26 October 2001) text available at: http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf (last visited May 2012).

[67] For more information on ownership vs. possession, *see* M. Turilli and L. Floridi, 'Cloud Computing and its Ethical Challenges', above note 53.

of creating universally accepted conventions for the cloud community.[68] Such a process could be initiated via a governmental entity or industry consortium, and if successfully implemented, could encourage portability between cloud services. At present, a number of such initiatives are being spearheaded by standards-development organizations, such as the Storage Networking Industry Association,[69] the Open Cloud Consortium,[70] the Object Management Group,[71] and the Distributed Management Task Force.[72]

Standardization comes with its own complexities and disadvantages. Not all established standards become universally accepted within a community. This presents a problem similar to that faced by a singular cloud-service provider seeking to choose one format over another for functional or business-driven purposes: how does a standard-setting organization determine which formats are most viable? Even within a single format, cloud providers may not universally utilize the technical aspects of the format.[73] Also, the market is constantly being shaped by non-standardized technologies, which can be both innovative and disruptive, some of which may be outside the scope of an established standard. As a result, the marketplace evolves and standards may be quickly displaced or become moot. Standards may even hinder further innovations by imposing obsolete requirements on developers. In this context, organic market evolution may be preferred over standardization. Rather than dictating which standards should be universal, the natural evolution of the market may cause industry players to gravitate naturally to the most useful infrastructure formats.

Technical distinctions in data and infrastructure designs are also a barrier to interoperability between EMR-system providers. Perhaps the problem for EMRs is more immediate, as the notion of data portability between different services and providers is inextricably linked with the maturation and development of a nationally and internationally coordinated EMR system. Standardization bodies are also hesitant to impose format standards for fear that such standards might impede innovation and future development.

More broadly speaking, there is currently no uniform approach that is best suited to encourage widespread interoperability within and between clouds. The development and adoption of open and well-documented formats, however, appears to be a prerequisite for the ultimate success of an interoperable cloud initiative. Openness aids developers in determining which standards are worth relying on as innovation progresses. The 'open' character of a format is not dependent on it being maintained by a standards organization; rather, open formats are generally unencumbered by intellectual property rights that limit their intended use and well documented for public use. Openness encourages collaboration and reuse between companies and across borders which raises the possibility for widespread (or universal) adoption across platforms. As the market matures, market participants may push for standardization of such an open format. In turn, this may help enable the conversion of data from a proprietary format into an open format between clouds, while still permitting the use of proprietary formats within individual cloud environments.[74]

---

[68] *See* Palfrey and Gasser, Interop, above note 4, Chapter 9: 'Getting to Interop', pp. 157-175.
[69] Storage Networking Industry Association (SNIA), http://www.snia.org (last visited May 2012).
[70] Open Cloud Consortium (OCC), http://opencloudconsortium.org (last visited May 2012).
[71] Object Management Group (OMG), http://www.omg.org (last visited May 2012).
[72] Distributed Management Task Force (DMTF), http://www.dmtf.org (last visited May 2012).
[73] Converting data from one cloud to another within the same format can still pose problems if cloud-service providers use different practices for handling a data format (e.g. metadata tags may be used for different purposes).
[74] This concept primarily relies on consensus among industry players and a technically viable, open, and well-

2. Legal and policy interoperability

Cloud-service providers and governments are aware of such discrepancies in privacy and security requirements between jurisdictions. Notably, many European governments complain, on behalf of their citizens, that US privacy laws need to be improved. The differing viewpoints between European end-users and their US counterpoints are starkly evident in their expectations of privacy protections. For instance, European end-users tend to see robust privacy protections as a means to facilitate the exchange of information, whereas US end-users tend to view privacy as a trade off to using online services.[75] As a consequence, there is a general fear that data hosted data in the US would be 'less safe' than data within European borders, regardless of the US-EU Safe Harbor agreement.[76]

Attempts at improving and, to a certain extent, harmonizing legal frameworks and policies may not solve this problem immediately. Although US regulators have been in the process of developing new privacy regulations and policy requirements for online services,[77] for instance, few new regulations have been enacted. At least in the short run, lawmakers seem hesitant to impose strict rules when market dynamics alter privacy concerns and expectations as end-users gravitate to new online services. Over time, however, governments may be more comfortable with imposing a series of 'baseline' privacy policy standards after the marketplace matures. For instance, many observers agree that transparency and disclosure of service-provider practices are a minimum requirement, so that end-users can have the tools to make decisions whether they want to use a particular service.[78]

---

documented formatting convention. If industry players can agree on a 'generic standard', it may be possible to standardize an open format for the purpose of transferring data between clouds. A cloud provider can convert a user's data from its closed proprietary format into this standardized 'intra-cloud format' which then allows the user to port his or her data to another cloud service without compromising the closed proprietary format. However, this approach may require additional policy initiatives to enforce (or at least encourage) these cloud-to-cloud sharing arrangements.

[75] *See e.g.* A. Liptak, 'When American and European Ideas of Privacy Collide', *New York Times*, February 27, 2010, p. WK1, available at: http://www.nytimes.com/2010/02/28/weekinreview/28liptak.html (last visited May 2012).

[76] J. Baker, 'EU Upset by Microsoft Warning About US Access to EU Cloud', *PCWorld*, 5 July 2011, available at: http://www.pcworld.com/article/235041/eu_upset_by_microsoft_warning_about_us_access_to_eu_cloud.html (last visited May 2012).

[77] The US legislative and executive branches have been actively proposing and debating legislation and regulations relating to Internet privacy issues. *See e.g.* The White House, 'Consumer Data Privacy in a Networked World: A framework for protecting privacy and promoting innovation in the global digital economy', 28 February 2010, available at: http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (last visited May 2012); The White House, 'Fact Sheet: Plan to Protect Privacy in the Internet Age by Adopting a Consumer Privacy Bill of Rights', 23 February 2012, available at: http://www.whitehouse.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b (last visited May 2012); FTC, 'FTC Issues Final Commission Report on Proecting Consumer Privacy', 26 March 2010, available at: http://www.ftc.gov/opa/2012/03/privacyframework.shtm (last visited May 2012); T. Vega and E. Wyatt, 'US Agency Seeks Tougher Consumer Privacy Rules', *New York Times*, 26 March 2012, p. A1, available at: http://www.nytimes.com/2012/03/27/business/ftc-seeks-privacy-legislation.html (last visited May 2012); Kerry-McCain Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Congress, 1st session (introduced in Senate, 12 April 2011) (no activity since 2011), bill text available at: http://epic.org/privacy/consumer/Commercial_Privacy_Bill_of_Rights_Text.pdf (last visited May 2012); 'Consumer Privacy Protection Act of 2011', H.R. 1528, 112 Congress, 1st session (introduced in House, 13 April 2011) (no activity since 2011), bill text available at: http://www.gpo.gov/fdsys/pkg/BILLS-112hr1528ih/pdf/BILLS-112hr1528ih.pdf (last visited May 2012).

[78] Body of European Regulators for Electronic Communications, 'BEREC Guidelines on Transparency in the scope of Net Neutrality: Best practices and recommended approaches', document no. BoR (11) 67, December 2011,

This leads to another complicating factor: the range of service agreements between end-users and online services.[79] These agreements represent a bargain between the user and the provider: in exchange for the use of cloud services, end-users assent to certain manipulations, some of which implicate privacy concerns such as disclosure to third parties. The value that cloud service providers are deriving from offering a 'free' service is the data inputs from the end-user, which are freely exchanged for the use of cloud services (i.e. with some form of consent). Some observers point out that this exchange reflects basic private ordering and the underlying business models of the user-provider relationship. This view arguably reflects the US notion of privacy protections in particular, when compared to European privacy standards, such as the EU's 1995 Data Protection Directive, which imposes restrictions on the transfer of data and on the ability of cloud service providers to manipulate end-user data.[80]

One approach to law enforcement issues are multilateral trade agreements. One suggestion is to create 'free trade zones' in which end-user data ownership dictates the applicable jurisdiction. For example, French end-user data that is stored in the US would be subject to French jurisdiction. This approach allows the interests of multiple countries to converge. However, this may create a 'race to the bottom' which encourages some countries to remain outside of these trade agreements so they can provide a 'safe haven' for cloud-service providers to eschew the application of more stringent jurisdiction—although globalization currently seems to cause a 'ratcheting up' of industry standards, whereby Internet companies strengthen individual privacy and security standards to meet the most stringent requirements in other countries.[81]

The effectiveness of multilateral agreements is often uncertain, given the lengthy political processes associated with the negotiation and execution of such arrangements.[82] In this light and looking at fast-moving nature of technological innovation, cloud experts are considering technical approaches that may be used to address jurisdictional concerns. The basic idea is that standards and policy approaches should be centered on incentivizing technical innovations that avoid or minimize adverse events (e.g. a data security breach).[83] In the healthcare context, for instance, technical innovations may mitigate security and privacy risks while also normalizing portability across EMR systems and healthcare providers. Technically and policy established security measures may aim to prevent access by unauthorized individuals, notify consumers of

---

available at: http://berec.europa.eu/doc/berec/bor/bor11_67_transparencyguide.pdf (last visited May 2012).

[79] *See* Bradshaw, 'Contracts for Clouds', above note 54; *see also* publications associated with Queen Mary University of London, Cloud Legal Project, 'Terms of Service Analysis for Cloud Providers', available at: http://www.cloudlegal.ccls.qmul.ac.uk/Research/researchpapers/37188.html (last visited May 2012).

[80] 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data', *Official Journal* L 281, 23 November 1995, pp.31-50, available at: http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm (last visited May 2012).

[81] This is similar to the effect discussed above in Section C, III, 1 'Technical interoperability and portability of data', where individual companies might choose to use a comprehensive practice that meets regulatory compliance in all jurisdictions, rather than attempting to tailor practices for each jurisdiction specifically.

[82] For example, the World Trade Organization's Agreement on Trade-related Aspects of Intellectual Property Rights (TRIPS) has been the subject of criticism for its complex negotiation framework and the resultingly vague terminology used to obtain consensus on sensitive issues. *See e.g.* P. Yu, 'TRIPS and its Achilles' Heel', *Journal of Intellectual Property Law*, vol. 18 (Spring 2011), pp. 479-531; P. Gerhart, 'The Tragedy of TRIPS'. *Michigan State Law Review*, vol. 2007 (2007), pp. 143-184.

[83] This process is sometimes referred to as 'technology dialectics'. *See e.g.* Latanya Sweeney, 'Constructing Provably Appropriate Technology', Data Privacy Lab, Fall 2006, available at: http://dataprivacylab.org/dataprivacy/projects/dialectics/index.html (last visited May 2012).

policy changes and data breaches, and ensure that privacy standards and expectations are being maintained on an extra-jurisdictional basis. Some US agencies, such as the FTC, are considering how to develop guidelines or rules that would attach certain disclosures or control levels to the EMR data itself—the idea is to start with a very broad framework which may be transferrable across multiple data streams and, over time, the framework and policies can become more granular as the risks and concerns become more easily identifiable.[84]

For example, as touched on in the context of the health data use case, prior to 2009's Health Information Technology for Economic and Clinical Health (HITECH) Act, HIPAA—the Health Insurance Portability and Accountability Act of 1996, which addresses, in part, the security and privacy of health data—did not specify any protections for data outside of US jurisdiction.[85] Health companies were therefore hesitant to engage in cross-border cloud usage for storing information that qualified as 'protected health information' under HIPAA.[86] With the HITECH Act, the relevant provisions of HIPAA were supplemented and it now requires organizations to secure protected health information 'by [using] a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals'.[87] Other provisions in this statute require these organizations to notify individuals when disclosure of such information is likely as a result of a breach.[88] The amendments in the HITECH Act incentivized a technical approach to risk mitigation by imposing encryption requirements and breach notifications. To some extent, these changes have facilitated multi-jurisdictional storage of highly sensitive data with minimal changes to existing policies. In this scenario, the hope is to minimize the consequences of a data breach, while encouraging companies to create new technologies to render health data unreadable. Economic incentives, like government reimbursement, may also aid the creation of technologies to address concerns that impact global interoperability.

E. Conclusion

In this article, we explored the phenomenon of cloud computing interoperability and approached the topic from both a theoretical and a practical (use case-based) perspective. The theoretical and practical observations presented suggest that cloud interoperability is a complex and rapidly evolving topic with great relevance for industry, consumers, and government, particularly from a law and policy perspective. Looking at the various levels and dimensions of interoperability, it seems safe to conclude that the multi-faceted interoperability issues are far from being resolved. Technological, legal, as well as economic barriers have yet to be broken down in order to create a highly interoperable cloud environment at an international scale, which can capitalize on the cost

---

[84] *See* proposed regulations, above note 77 and accompanying text.

[85] US Department of Health & Human Services,'Understanding Health Information Privacy', available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html (last visited May 2012).

[86] The State of Nevada Department of Health and Human Services Office of Health Information Technology, 'State Health Information Technology – Strategic and Operational Plan', 23 May 2011, available at: http://dhhs.nv.gov/PDFs/HIT/NV_StaeHITPlan_AppendixG.pdf (last visited May 2012).

[87] HITECH Act of 2009, 42 U.S.C. § 17932(h)(1)(B) found in Public Law 111-5, 123 Stat. 261-262, available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf (last visited May 2012). *See also* 'Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, Or Indecipherable to Unauthorized Individuals', Fed. Reg. 74, 27 April 2009, p.19009, available at: http://www.nacua.org/documents/HHSGuidance_SpecifyingTechnologiesMethodologiesRenderPHIUnusable.pdf (last visited May 2012).

[88] *See* HITECH Act, above note 87, § 17932(a).

savings, efficiencies, and innovations promised by the cloud, while also mitigating its risks, including privacy, security, and other concerns.

Further, both the theoretical and practical observations suggest that cloud interoperability is an issue full of nuances which require in-depth analysis, not only when looking at possible solutions, but even when identifying the problems. In this process, market forces will play a key role in determining the appropriate levels of cloud interoperability—for instance through technical standard setting. That being said, observations from theory and practice also highlight the important role of governments, especially in the realm of technical interoperability and, most prominently, in the context of legal and policy interoperability. With regard to technical interoperability, we already see the productive role governments can play in their function as conveners and facilitators of standard setting processes as well as through their use of procurement power.

As far as legal and policy interoperability is concerned, governments can—and should—make several contributions to set the stage for increased cloud computing interoperability. From a practical perspective, four contributions will be decisive. First, states will need to play a key role in clarifying the interpretation of current laws and regulations as they apply to cloud computing, hence reducing uncertainty across jurisdictions. Second, governments can address the problem of transparency by improving clarity and communication regarding legal norms and thus contribute to the fostering of legal interoperability. Third, state actors can engage in efforts to harmonize certain areas of law—or at least basic underlying principles, as in the case of privacy, for instance—to enhance the working together of legal norms across jurisdictions. Finally, governments can engage in the development of new institutional designs to bridge differences in legal regimes but still enable the global flow of data in the age of cloud computing (e.g. the US-EU Safe Harbor agreement is an illustration of this idea).

Despite the important role the government can play in addressing cloud interoperability, the theoretical framework sketched in this article as well as the practical observations make clear that cloud interoperability at its various levels ultimately remains a collective challenge, one which needs to be addressed by all stakeholders on a global scale by using the various tools that are available, including by facilitating private ordering, promoting technical and legal standard-setting, and leveraging the procurement and convening power of governments, where appropriate. As such, cloud interoperability itself depends on the collaboration among users, cloud providers, intermediaries, and governments.