10-1-2013

# *Facilitando the Cloud*: Data Protection Regulation as a Driver of National Competitiveness in Latin America

Horacio Gutiérrez

Daniel Korn

# *Facilitando* the Cloud: Data Protection Regulation as a Driver of National Competitiveness in Latin America

Horacio E. Gutiérrez[1] & Daniel Korn[2]


I. Cloud Computing is Increasing the Importance of Balanced Data Privacy Rules ..... 35 R
II. Fostering Increased National Competitiveness Requires a Balanced Data Protection Regulatory Framework for Cloud Computing .... 39 R
A. *Benefits of the Cloud* ..... 39 R
1. Job Creation Through Innovation ..... 39 R
2. Cost Savings ..... 40 R
3. Democratization of Computing and Social Inclusion ..... 42 R
4. Increased Agility ..... 43 R
5. Security ..... 45 R
B. *An Important Role for Balanced Regulation* ..... 46 R
1. Ensuring Privacy Protection ..... 46 R
2. Encouraging Greater Transparency ..... 47 R
3. Enabling and Protecting Cross-Border Data Flows ..... 48 R
4. Harmonization of Data Protection Rules and Interoperability ..... 51 R
5. Strengthening Laws Against Cybercrime .... 53 R
III. Challenges, Trends, and the Early Experience of Cloud Regulation ..... 53 R
A. *Cloud Computing Presents Important Privacy and Data Security Questions* ..... 54 R
B. *Regulatory Trends* ..... 55 R
C. *Microsoft's Approach* ..... 56 R
IV. Conclusion ..... 61 R


Investments in Internet infrastructure throughout Latin America are beginning to pay off, particularly as consumers,

1. Corporate Vice President and Deputy General Counsel, Microsoft Corporation. Mr. Gutiérrez is the "2013 Lawyer of the Americas" named by the University of Miami School of Law's *Inter-American Law Review*.

2. Director of Corporate Affairs, Microsoft Latin America.

businesses, government agencies, health care providers and educational institutions use Internet connections to access innovative cloud computing services.[3] Indeed, the market for cloud computing in Latin America is expected to grow at an annual rate of 70 percent from 2012-16.[4] This is not surprising, as cloud computing enables users with an Internet connection to affordably access a level of computing power that until recently was available only to companies with large IT budgets and in-house expertise.[5] Most importantly, this technology has enormous potential to create new jobs, drive down costs, and promote social inclusion.[6]

The above notwithstanding, however, adoption of cloud computing in Latin America is at an early stage, and decisions taken today by policymakers and other stakeholders will influence the degree to which the citizens of particular nations and in the region as a whole will benefit from this technology in the short to medium term. Twenty-first century data protection rules and policies, and whether they are designed with the flexibility to accommodate this transformative technology, will play an important role in facilitating cloud computing adoption and the benefits it produces for *national competitiveness*, *i.e*. the economic growth and long-term improvement of a society's standard of living resulting from improvements in national productivity and efficiency.[7] Policymakers throughout the region must avoid the easy road and be ready instead to make the often-tough political decisions necessary to develop data protection rules that will allow

3. "Cloud computing" can be defined as a model for convenient on-demand network access to computing resources that are in a shared pool and can be rapidly delivered with minimal management effort or service provider interaction. *See The NIST Definition of Cloud Computing*, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

4. *See Latin American cloud computing worth US $280mn in 2012, says IDC*, START UP IN BRAZIL (Sept. 4, 2012), http://startupbrazil.co.uk/latin-american-cloud-computing-worth-us280mn-2012-idc/.

5. *See generally* Alexa Huth & James Cebula, *The Basics of Cloud Computing*, U.S. COMPUTER EMERGENCY READINESS TEAM, *available at* http://www.us-cert.gov/sites/default/files/publications/CloudComputingHuthCebula.pdf (explaining how cloud computing is an easily accessible resource for individuals and businesses).

6. *See* Joe McKendrick, *Cloud Will Generate 14 Million Jobs by 2015: That's a Good Start*, FORBES (Mar. 5, 2012, 8:21 PM), http://www.forbes.com/sites/joemckendrick/2012/03/05/cloud-will-generate-14-million-jobs-by-2015-thats-a-good-start/.

7. Orlando Ayala, *Defining National Competitiveness*, FUTURE GOV (May, 20, 2011), http://www.futuregov.asia/articles/2011/may/20/defining-national-competitiveness.

their countries to take the lead in the emerging era of cloud computing for the benefit of their citizens.

This article examines how governments and industry in the region can build consumer confidence in the cloud through balanced and consistent data protection rules and thereby increase a country's national competitiveness. Part I examines how data privacy rules can empower cloud computing. Part II explores the tremendous benefits that cloud computing presents for national competitiveness. Part III highlights regulatory challenges posed by cloud computing, including the early experience of cloud regulation and the role that industry plays in establishing customer trust in the cloud, closing specifically with a description of Microsoft's approach to these issues.

## I. CLOUD COMPUTING IS INCREASING THE IMPORTANCE OF BALANCED DATA PRIVACY RULES

Privacy concerns existed long before the cloud, the Internet, or even computers. For centuries, people have sought to control the use and disclosure of their personal details.[8] Today, many governments around the world are evaluating the need for laws that will keep up with the requirements and realities of cloud computing while achieving the same benefits that long have driven privacy legislation: empowering individual decisions regarding privacy, maintaining information security, and building confidence in a major advance in technology that promises to transform society for the better if managed correctly. In Europe, Digital Agenda Commissioner Neelie Kroes has urged the adoption of "clear and cloud-friendly rules . . . [because] a 'cloud' without clear and strong data protection is not the sort of cloud we need."[9] Likewise, the U.S. Department of Commerce recently observed that the ability to "safely use services such as cloud-based email and file storage to their full potential depends on privacy protections that are consistent with other computing models."[10] We agree. Put

8. *See, e.g.*, ROBERT ELLIS SMITH, BEN FRANKLIN'S WEBSITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET, (Privacy Journal, 2004) (discussing Americans' desire for privacy throughout the history of the United States).

9. Neelie Kroes, Vice-President for the Digital Agenda, Eur. Comm'n, Speech at Les Assises du Numérique conference: *Cloud Computing and Data Protection* (Nov. 25, 2010), *available at* http://europa.eu/rapid/press-release_SPEECH-10-686_en.htm.

10. *See* Department of Commerce Internet Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (December

simply, it is in the collective interest of all stakeholders that cloud users have well-founded confidence in the cloud.

In Latin America, interest in data protection likewise is on the rise.[11] Since the 1980s, many governments in Latin America have provided a constitutional right for individuals to access and correct their personal data. Also known as "habeas data," this protection is intended "to safeguard individual freedom from abuse in the information age."[12] Habeas ensures "a real control over sensible personal data, stopping the abuse of such information, which will be detrimental to the individual."[13] Because these habeas data provisions typically are in national constitutions, they receive "the highest level of protection possible, and faster procedures and better courts usually accompany it."[14] For instance, Section 43(3) of Argentina's constitution provides a strong habeas right:

> Any person shall file this action to obtain information on the data about himself and their purpose, registered in public records or data bases, or in private ones intended to supply information; and in case of false data or discrimination, this action may be filed to request the suppression, rectification, confidentiality or updating of said data. The secret nature of the sources of journalistic information shall not be impaired.[15]

Since 2000, countries in Latin America are passing comprehensive data protection laws that are modeled after Europe's Data Protection Directive from 1995.[16] These laws vary widely, but they generally contain pre-cloud restrictions on the use and transfer of data, require express consent of the data subject before processing, allow individuals to access and correct every possible iteration

---

2010), *available at* http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf.

11. *See* Aldo M. Leiva, *Data Protection Law in Spain and Latin America: Survey of Legal Approaches*, 41 INT'L LAW NEWS 4 (2012), *available at* http://www.americanbar.org/publications/international_law_news/2012/fall/data_protection_law_spain_latin_america_survey_legal_approaches.html.

12. ENRIQUE FALCÓN, HÁBEAS DATA: CONCEPTO Y PROCEDIMIENTO 28 (1996).

13. Andrés Guadamuz, *Habeas Data vs. the European Data Protection Directive*, 3 J. INT'L T.5 (2001).

14. *Id.*

15. Art. 2, CONSTITUCIÓN NACIONAL (Arg.), *authors' translation*.

16. Leiva, *supra* note 11 ("Spanish and Latin American approaches to personal data protection are rooted in the European concept of personal privacy rights that have developed throughout Europe for several decades and have culminated via regional integration in adoption of the European Data Protection Directive (the 'Directive') in 1995.").

of their personal data, and mandate steps to protect data security. In 2000, Argentina enacted the region's first comprehensive data protection law, which shared many elements of the European Union's pre-cloud 1995 directive.[17] Uruguay adopted a very similar data protection law years later.[18] Beginning with Mexico's landmark law in 2010, consideration, and often adoption, of comprehensive data protection laws has become the norm in Latin America, as illustrated in the chart[19] below.

| Country | Key Points |
|---|---|
| Argentina | 1. Argentina adopted an EU-style law in 2000 and received an adequacy determination from the EC in 2003.<br>2. As a general matter, international data transfers from Argentina are prohibited unless the data subject grants prior express consent if the destination country does not have what the Argentine regulator deems to be "adequate" laws. No "safe harbor" has been established to facilitate data flows to countries not deemed to be "adequate." |
| Brazil | 1. Brazil does not have a comprehensive data protection law, although as in many countries in the region there is a general constitutional right to privacy. The Ministry of Justice drafted a bill and sought public comment on it in 2011. More recently, the Brazilian Congress is considering a bill that would allow the President to require personal data of Brazilian citizens to be kept in the country. |
| Chile | 1. Chile adopted a data protection law in 1999, but it is not considered "comprehensive" in nature.<br>2. In January 2012, the executive branch presented a proposed Bill of Law to the Chilean Congress, aiming to create a comprehensive data protection law. In November 2013, the Bill was still in Congressional committee. |
| Colombia | 1. Colombia adopted a comprehensive data privacy law, with final action taken in October 2012 when Law 1581 was enacted.<br>2. Similar to laws in Argentina and Uruguay, the new law prohibits transfer of data across borders to countries that do not have "adequate" data protection regimes as determined by the Colombian regulator, unless the data subject grants prior express consent. Secondary legislation, Decree 1377, was issued in June 2013. |
| Costa Rica | 1. Costa Rica adopted a comprehensive data privacy law in September 2011. Among other requirements, in general personal data cannot be processed without the express consent of the data subject.<br>2. In March 2013, the Ministry of Justice and Peace issued regulations under the new law. Most unusually, the regulations would require data controllers to provide an all-access "Super User" account to the data protection authority.<br>3. A Presidential circular issued on May 15, 2013 specifically promotes cloud procurement in the public sector. |

17. Law No. 25326, Oct. 30, 2000, (Arg.).

18. L. 18.331, 11 de agosto, 2008, DIARIO OFICIAL (Urug.).

19. This chart was prepared by Matt DelNero of Covington & Burling LLP on Nov. 8, 2013.

| | |
|---|---|
| Dominican Republic | 1. On April 22, 2013, the Dominican Republic's Senate passed a Data Protection bill further to Article 44.2 of the Dominican Republic's Constitution. The bill is currently pending passage in the Lower House.<br>2. The bill follows many of the principles and concepts found in the EU Data Protection Directive, such as limitations on the transfer of data, special protection for sensitive data, and creation of an independent data protection authority. It also requires parental consent for processing of data on children younger than the age of 16. |
| Mexico | 1. Mexico adopted landmark data privacy legislation in 2010. Regulations pursuant to the law were issued in December 2011.<br>2. The Mexican law may provide a "third way" between the ad hoc approach prevailing in the United States and the more prescriptive approach favored in Europe and, increasingly in many countries in Latin America. For example, the law provides more flexibility in international data transfer. In addition, the law embraces the consent principle but makes clear that in many cases, consent may be obtained tacitly through proper disclosures in a privacy notice.<br>3. Mexico has embraced the data protection principles of the Asia Pacific Economic Cooperation forum (APEC) instead of the more restrictive EU data protection framework. In addition to APEC elements found in the law, as of January 2013, Mexico became the second formal participant (following the U.S.) in the APEC Cross-Border Privacy Rules framework.<br>4. New guidelines on privacy notices went into effect on April 17, 2013. Similar to rules in the EU, the new guidelines require controllers to provide sufficient notice and obtain consent before personal data is collected using cookies, web beacons, or other automated means. |
| Nicaragua | 1. Nicaragua adopted a comprehensive data protection law in March 2012.<br>2. The new law largely follows an EU-based model. It also includes concepts such as a "right to be forgotten," which refers to a right to have all traces of one's data deleted from a company's records. |
| Peru | 1. Peru's data protection law adopted in 2011 mostly follows the EU model, but with somewhat more modern means of enabling the data flows that are crucial to cloud computing. Specifically, while the default rule requires consent to transfer data to countries without "adequate" data protection laws, the controller can overcome this obstacle if it takes steps to make itself accountable for the protection of the data once it is transferred outside of the country.<br>2. Peru adopted regulations pursuant to the law by decree on March 22, 2013. The Regulation includes a provision on cloud computing (referred to as "*tratamiento de datos personales por medios tecnológicos tercerizados*" – phrasing intended as a technologically neutral description allowing for as yet unknown technological developments in the future). The provision allows controllers to rely upon third-party cloud services so long as they ensure that the cloud provider complies with the data protection requirements of the law. In addition, the cloud services provider itself should be made accountable under the contract with the controller. |
| Uruguay | 1. Uruguay adopted an EU-style law in 2008 and received an adequacy determination from the EC on Aug. 21, 2012.<br>2. International data transfers from Uruguay are prohibited if the destination country does not have "adequate" laws. Yet unlike its Argentine counterpart, the Uruguayan DPA has issued a resolution recognizing as "adequate" any destination country deemed adequate by the EU. We understand that this resolution has been interpreted to permit transfer to any organization certified under the U.S. /EU safe harbor. |

## II. Fostering Increased National Competitiveness Requires a Balanced Data Protection Regulatory Framework for Cloud Computing

The cloud provides pooled computing resources that are available on demand and accessible from any Internet-connected device at any time.[20] Cloud service providers operate a global network of data centers to provide seamless service to a worldwide customer base.[21] This section outlines the key economic benefits of cloud computing and outlines elements of a balanced regulatory framework that could help promote consumer adoption and growth of this remarkable technology to the community's benefit.

### *A. Benefits of the Cloud*

Few recent technologies have presented more potential economic benefits than the cloud. By 2014, the worldwide market for cloud computing is expected to grow to $150 billion.[22] Particularly in emerging markets, cloud computing could become an engine for economic growth and social benefits.[23] The cloud offers both developed and emerging economies a wide range of benefits. Each benefit we describe below should be of particular interest to small- and medium-sized entities (SMEs), which employ an estimated 67 percent of the workforce in Latin America and in many cases have not been able to leverage significant computing power until today.[24]

#### 1. Job Creation Through Innovation

Cloud computing has the potential to create jobs through local innovation. This is largely because cloud computing's lowering of the need for major technology investments and the cost of ongoing maintenance for legacy applications and infrastructure, frees company budgets for devotion to *new markets* and *new products*, both

20. *See* Huth, *supra* note 5.

21. *Id.*

22. Andrew R. Hickey, *Cloud Computing Services Market To Near $150 Billion in 2014*, CRN (June 22, 2010, 12:46 PM), http://www.crn.com/news/managed-services/225700984/cloud-computing-services-market-to-near-150-billion-in-2014.htm.

23. *See With Cloud, SMBs Will Lead Emerging Economies Across the Digital Divide*, Cisco (Sep. 2012), http://www.cisco.com/web/about/ac79/docs/FastFacts/FastFacts_Cloud-and-Digital-Divide.pdf.

24. Angel Gurría, *Latin American Economic Outlook 2013: SME Policies for Structural Change* (OECD 2012), *available at* http://www.keepeek.com/Digital-Asset-Management/oecd/development/latin-american-economic-outlook-2013_leo-2013-en.

of which lead to job growth.[25] Indeed, in regards to the information technology sector in particular, experts expect cloud computing to be the engine of job growth in the next decade. According to a November 2012 IDC White Paper sponsored by Microsoft, the global demand for cloud-related jobs will grow by 26 percent annually through 2015, creating as many as 7 million cloud-related jobs worldwide.[26] Through 2015, cloud-related jobs will increase at an annual rate of 22 percent in North America and 24 percent in Europe, while the emerging markets of Latin America, Central and Eastern Europe, the Middle East, and Asia Pacific will see the greatest rate of cloud-related job growth: 34 percent annually.[27]

Millions of these new jobs are exactly the type of high-skilled, high-paying positions that governments are eager to attract. For instance, in a study published by the Economic Commission for Latin America and the Caribbean (ECLAC or CEPAL (in Spanish)), analysis by the economists Andrea Colciago and Federico Etro found that adoption of cloud computing by businesses in Brazil could result in the creation of 900,000 new jobs.[28] Similarly, the Mexican Institute for Competitiveness (IMCO) recently found that with cloud technology Mexico can create 1,800 new small and medium companies, employing in the aggregate an estimated 63,400 employees. This is based on a conservative estimate of savings of just one percent of companies' fixed costs due to the benefits of the cloud.[29]

## 2. Cost Savings

In addition to creating high-quality jobs, cloud computing

25. *See, e.g.*, Mohana Ravindranath, *Analysts expect growth in cloud jobs*, WASH. POST (Aug. 15, 2013, 8:00 AM), http://www.washingtonpost.com/business/on-it/analysts-expect-growth-in-cloud-jobs/2013/08/14/56d5715a-04fb-11e3-a07f-49ddc7417125_story.html ("Across industries, cost-saving associated with switching to cloud computing has "translated not into job loss, but more available resources to invest in other aspects of the business. . .").

26. Cushing Anderson & John F. Gantz, *Climate Change: Cloud's Impact on IT Organizations and Staffing*, IDC 1, 3 (Nov. 2012), http://www.microsoft.com/en-us/news/download/presskits/learning/docs/idc.pdf.

27. *Id.* at 4-5.

28. *See* Valeria Jordán et al., *Banda Ancha en América Latina: Más allá de la Conectividad*, CEPAL 1, 29 (Feb. 2013), http://www.cepal.org/publicaciones/xml/2/49262/BandaAnchaenAL.pdf.pdf.

29. "*Computo en la Nube": Nuevo Detonador para la Competitividad de México*, INSTITUTO MEXICANO PARA LA COMPETITIVIDAD A.C. (IMCO), "Computo en la Nube": Nuevo detonador para la competitividad de México, at) 1, 31 (May 2012), http://imco.org.mx/images/pdf/Computo_en_la_Nube-detonador_de_competitividad_doc.pdf [hereinafter IMCO Cloud Report].

boosts the economy by providing businesses and government agencies with significant savings on information technology services and infrastructure.[30] Recent data suggest that hybrid cloud deployment would reduce total IT spending by approximately 20 percent to 30 percent.[31] Because any business or organization can connect to the full benefits of the cloud with a simple Internet connection, there is minimal need for upfront capital investments. Previous generations of technology required significant investments in servers and other physical equipment, but such capital is unnecessary with cloud computing. By aggregating demand for computing, the cloud allows server utilization rates to increase. IMCO estimates that the public sector in Mexico can save 1.7 percent of its annual expenditures by moving to the cloud.[32] Of particular note is that these cost savings serve to increase the democratization of computing which leads to greater social inclusion, as further discussed in the next section.

Moreover, large-scale data centers result in lower costs per server because they require less electricity to operate.[33] And increasing the number of customers lowers the application management and server cost per tenant. In a traditional, non-cloud enterprise, a single system administrator can service approximately 140 servers.[34] In contrast, a cloud center typically runs thousands of servers at a time that are capable of handling many tasks at once.[35] This efficiency allows IT employees to focus on higher value-add activities like building new capabilities and addressing user requests.

The corresponding energy savings could also translate into reduced carbon emissions, as a result of which cloud computing

30. *See* Hilary Kramer, *Washington Moves Into the Cloud: Saving Money and Securing Data*, FORBES (July 8, 2013, 6:45 AM), http://www.forbes.com/sites/hilarykramer/2013/07/08/washington-moves-into-the-cloud-saving-money-and-securing-data/.

31. *Business Agility and the True Economics of Cloud Computing*, VMWARE 1, 6 (2011), https://www.vmware.com/files/pdf/accelerate/VMware_Business_Agility_and_the_True_Economics_of_Cloud_Computing_White_Paper.pdf.

32. IMCO Cloud Report, *supra* note 29, at 34.

33. *See, e.g.*, Yuan Yao et al., *Data Centers Power Reduction: A Two Time Scale Approach or Delay Tolerant Workloads* (2012), http://www.eecs.berkeley.edu/~huang/data-center-power-infocom12.pdf (discussing how large-scale data centers have the potential to reduce power costs).

34. *See* Rich Miller, *How Many Servers Can One Admin Manage?*, DATA CENTER KNOWLEDGE (Dec. 30, 2009), http://www.datacenterknowledge.com/archives/2009/12/30/how-many-servers-can-one-admin-manage/.

35. *See* Clair Cain Miller & Quentin Hardy, *Google Elbows Into the Cloud*, N.Y. TIMES (Mar. 12, 2013), http://www.nytimes.com/2013/03/13/technology/google-takes-on-amazon-and-microsoft-for-cloud-computing-services.html?pagewanted=all.

has been called "Green IT."[36] IMCO estimates that Mexico's medium and large sized business sector would in the aggregate reduce carbon emissions equivalent to removing 90,000 cars from circulation by migrating to the cloud.[37]

### 3. Democratization of Computing and Social Inclusion

Cloud computing not only increases efficiency; it also increases equality. By providing access to a level of computing power once available only to large corporations and developed economies, the cloud is the next stage in the democratization of computing and increasing social inclusion.[38] With cloud computing, organizations of any size and in virtually any location can tap into supercomputing power and software applications that previously were available only to the largest global companies.[39] People also can build entirely new computing tools in the cloud. For instance, cloud computing allows employees at rural hospitals to consult with specialists worldwide in real time, providing rural residents with medical care that they never would have been able to receive before the cloud.[40] The cloud also reduces hospitals' costs of storing X-rays and other voluminous health records.[41] Indeed, cloud computing at hospitals is expected to grow at a compound annual rate of 20.5 percent between 2012 and 2017.[42]

Similarly, the cloud has presented unprecedented opportunities to rural and low-income school districts.[43] The cloud provides schools with powerful web-based applications, distance learning, and low-cost storage.[44] It also allows small schools to access educational materials that they otherwise would never have. Moreover, the cloud allows governments to take a giant leap forward in the

36. IMCO Cloud Report, *supra* note 29, at 40.

37. *Id.*

38. Joe Mullich, *16 Ways the Cloud Will Change Our Lives*, WALL ST. J. (Jan. 7, 2011), http://online.wsj.com/ad/article/cloudcomputing-changelives.

39. *See generally* Huth, *supra* note 5.

40. Pam Belluck, *Nantucket Hospital Uses Telemedicine as Bridge*, N.Y. TIMES, (Oct. 8, 2012), http://www.nytimes.com/2012/10/09/health/nantucket-hospital-uses-telemedicine-as-bridge-to-mainland.html?pagewanted=all.

41. Ken Terry, *Cloud Computing in Healthcare: The Question Is Not If, But When*, FIERCEHEALTHIT (Jan. 9, 2012), http://www.fiercehealthit.com/story/cloud-computing-healthcare-question-not-if-when/2012-01-09.

42. Bernie Monegain, *3 Big Trends for the EHR Cloud*, Healthcare IT News (Oct. 8, 2012), http://www.healthcareitnews.com/news/3-big-trends-ehr-cloud.

43. *See* KerriLee Horan, *Saved by the Cloud*, DISTRICT ADMINISTRATION (Feb 2010), http://www.districtadministration.com/article/saved-cloud.

44. Diane Weaver, *Six Advantages of Cloud Computing in Education*, PEARSON (Apr. 2013), http://www.pearsonschoolsystems.com/blog/?p=1507.

offer of citizen services. For instance, Puerto Rico-based Rock Solid developed a cloud-based Citizen's Service hotline for the government of Panama, which allows Panama residents to dial 3-1-1 to reach a centralized service that directly connects them with government agencies.[45] Similarly, Colombia's education system has used the cloud to improve student standardized testing.[46] Without this technology, the Colombian Institute for Educational Evaluation (ICFES) would have required thousands of its own servers to make these results available to students two times per year.[47] By using cloud computing, ICFES took advantage of the scale and on-demand nature of the cloud, saving on servers to meet this demand. This benefitted the government as well as the students, parents, and teachers.

What we're most passionate about is that the economics of cloud computing represents the bringing down of a major wall that divided our societies between those that *could* make the major capital cost investment required to access and update the latest software technologies that are increasingly required for business, and those that couldn't make that investment. With the lower price point for access to cloud computing, that unhappy distinction will largely fade away and regular interaction with the latest software should become much more of a reality to the larger community.

### 4. Increased Agility

Cloud computing also allows businesses and government organizations to agilely adapt to new demands and challenges. Unprecedented computing power and storage capacity now available in the cloud allows organizations to roll out new applications and services with significantly greater speed—and less risk—than in the past.[48] Services that once would have required large capital investments and lengthy deployments can be launched in a matter

45. *See* video at Rock Solid Technologies, *Dynamics CRM & Rock Solid Republic of Panama-311 System*, YOUTUBE (Apr. 6, 2011), http://www.youtube.com/watch?v=HVUCALNG2D4.

46. Hernán Rincón, *This is Latin America's Decade: The Cloud Will Make it Possible*, AMERICAS QUARTERLY (Fall 2011), http://www.americasquarterly.org/node/3085.

47. *Id.*

48. *See, e.g.*, Reuven Cohen, *Build Your Own Web or Mobile App In Minutes With These Cloud Based Tools*, FORBES (Mar. 22, 2013), http://www.forbes.com/sites/reuvencohen/2013/03/22/build-your-own-web-or-mobile-app-in-minutes-with-these-cloud-based-tools/ (explaining how the cloud can be used by companies to quickly create applications).

of weeks or even days. In the past, when businesses experience sudden surges in popularity, their web and internal servers were often unable to handle the increased demand. When Costa Rica's devastating earthquake on September 5, 2012 crippled traditional communications such as telephones, radios, and televisions, residents were able to obtain information by visiting the website of the national television station (Teletica) since the website was hosted in the cloud, and the internet capacity of the website could be scaled up in order to meet the surge in demand.[49] With cloud computing, businesses could easily adjust to such increased demand because they are not limited to the capacity of their internal servers. According to a survey of corporate decision makers conducted by AbsolutData for VMware in February 2011, 65 percent of respondents believe that the cloud plays a "key role" in increasing agility and that cloud computing "could help their organizations maintain a flexible architecture to support changes."[50]

This flexibility is largely due to the mobility of the cloud. It not only provides a different kind of access than we've had in the past; it is also a far more widespread kind of access. More than three-quarters of the world's population has access to a mobile phone.[51] Mobile phones are very different from the PCs on our desk, or even our laptops. They are phones, texting tools, still cameras, movie cameras, computers, web portals, gamepads, and yet they are still small enough to fit in our shirt pockets. We carry them everywhere we go for always-on, always-connected two-way access to the digital world. Mobility is changing how data and services are accessed just as the web changed how data and services are delivered and just as cloud computing is changing how they're processed and managed. For instance, a new mobile app named "Agentto" developed in Brazil helps make communities safer by providing individuals with a real time, location-based channel for notifying family, friends and the authorities during critical situations such as accidents, health problems, domestic violence, kidnappings, and catastrophes.[52]

49. Mark Lyndersay, *Microsoft Evangelises the Cloud*, TRINIDAD & TOBAGO GUARDIAN (Oct. 25, 2012), http://www.guardian.co.tt/business-guardian/2012-10-24/microsoft-evangelises-cloud.

50. VMware, *Business Agility and the True Economics of Cloud Computing*, *available at* https://www.vmware.com/files/pdf/accelerate/VMware_Business_Agility_and_the_True_Economics_of_Cloud_Computing_White_Paper.pdf.

51. *Mobile Phone Access Reaches Three Quarters of Planet's Population*, WORLD BANK (July 17, 2012), http://www.worldbank.org/en/news/press-release/2012/07/17/mobile-phone-access-reaches-three-quarters-planets-population.

52. AGENTTO, https://agentto.com/About.aspx (last visited Sept. 28, 2013).

## 5. Security

Although many organizations and individuals are understandably concerned about cloud security, in reality there is no technical reason why the cloud cannot be as secure—if not more so—than traditional computing. In a 2012 study of 70,000 security breaches at 1,600 companies, AlertLogic found that on-premises computing systems were more vulnerable to attacks than cloud applications.[53] Forty-six percent of corporate servers were hit with "brute force" attacks, compared to 39 percent of cloud systems.[54]

As the European Network and Information Security Agency (ENISA) has recognized, "cloud computing has significant potential to improve security and resilience."[55] While robust data privacy rules are essential to give users confidence that their data is safe in the cloud, cloud technologies can themselves enhance the security and privacy of data—particularly for small and medium enterprises that have only limited information security resources and expertise. Many smaller companies do not have the resources to deploy robust physical and technical security controls, systematically apply and test security patches, implement comprehensive encryption solutions, or achieve information security and privacy certifications. Cloud computing allows these smaller organizations to achieve the same safeguards available to larger organizations with sizeable information technology budgets, staff, and facilities.[56]

In light of all of these benefits, it is not surprising that users are enthusiastic about the cloud. For example, KPMG found that an overwhelming 59 percent of Dutch decision-makers and business leaders agree that "cloud computing is the future model of IT."[57] The majority of consumers and business leaders believe

53. Joe McKendrick, *Cloud Apps Somewhat More Secure Than On-Premises Apps: Survey*, FORBES, (Sept. 19, 2012), http://www.forbes.com/sites/joemckendrick/2012/09/19/cloud-apps-somewhat-more-secure-than-on-premises-apps-survey/

54. *Id.*

55. *FAQ's to the report "Cloud Computing: Benefits, risks and recommendations for information security,"* EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY (ENISA) (last visited Sep. 19, 2013), http://www.enisa.europa.eu/media/faq-on-enisa/FAQ%20Cloud%20Computing.pdf.

56. *See* Tom Kelly, *SMEs must embrace the cloud to achieve global growth*, THE GUARDIAN (Apr. 26, 2013), http://www.theguardian.com/media-network/media-network-blog/2013/apr/26/cloud-services-sme-businesses-growth?guni=Article:in%20body%20link.

57. KPMG, FROM HYPE TO FUTURE: KPMG'S CLOUD COMPUTING SURVEY (2010), *available at* http://www.kpmg.com/ES/es/ActualidadyNovedades/ArticulosyPublicaciones/Documents/2010-Cloud-Computing-Survey.pdf.

these technologies can help government operate more efficiently and effectively as well. The challenge for the cloud industry is to harness this excitement and assure business and individual customers that their data is secure on the cloud.

### *B. An Important Role for Balanced Regulation*

Regulators can help extend the benefits of cloud computing to more enterprises and individuals by establishing trust in cloud computing, ensuring privacy and data security, and resolving legal and public policy uncertainties. This section outlines the general elements of a data protection and privacy regulatory framework that promotes national competitiveness in cloud computing.

#### 1. Ensuring Privacy Protection

The cloud will not realize its full potential if users do not trust the technology. Numerous surveys show that businesses and individuals continue to have significant concerns about the privacy and security of the cloud. For example, a 2010 survey by the World Economic Forum found that 90 percent of respondents in Europe see privacy as a "very serious" constraint on adopting cloud computing.[58] As people and organizations around the world move information from desktops to their mobile devices and into the cloud, they want to know that their data will remain safe and protected.

Regulators can help ensure that users, both businesses and individuals, do not lose privacy protections in moving data to the cloud by providing a clear and fair regulatory framework. As Microsoft General Counsel Brad Smith stated at the 34th Annual Conference of Data Protection and Privacy Commissioners held in Uruguay in October 2012, "We need clarity so that everybody knows what they need to do, and that companies that act responsibly are not going to find themselves suffer at the hands of companies who do not, and regulation creates that floor that provides that level playing field."[59] The regulatory framework should focus

58. Joanna Gordon et al., *Exploring the Future of Cloud Computing: Riding the Next Wave of Technology-Driven Transformation*, WORLD ECONOMIC FORUM (2010), *available at* http://www3.weforum.org/docs/WEF_ITTC_FutureCloudComputing_Report_2010.pdf.

59. Brad Smith, General Counsel and Executive Vice President, Microsoft Corp, Keynote Address at the 34th International Conference of Data Protection and Privacy Commissioners: Putting People First: Moving Technology and Privacy Forward

on the ultimate goals of ensuring data security, protecting consumer privacy, and building trust in the cloud.

But we don't need rules of the road from regulators alone. Industry self-regulation and market-based innovation will also be key to ensuring privacy protection. Self-regulation in the form of industry standards can move technology forward faster and more globally than regulation alone is able to do. For example, interested stakeholders have developed a draft international standard, ISO/IEC 27018, by which a cloud provider can demonstrate to customers and regulators that it handles personal data properly and otherwise ensures the confidentiality, integrity and availability of that data.[60] Likewise, with market-based innovation, there is an opportunity for companies to experiment, to try new things, to see what consumers want, and if consumers do, in fact, want what companies are offering, there is an opportunity for those companies to grow.

### 2. Encouraging Greater Transparency

Similarly, a data protection regulatory framework can provide *customers* with much-needed information about the cloud. It is not enough for cloud providers to claim that their services are private and secure. Customers should be informed in detail why this is so. Privacy and data security regulations can require cloud service providers to maintain comprehensive written information about their security programs and safeguards, provide summaries of those programs to customers, and disclose their privacy practices to any customer from whom personal information is collected.

Transparency is especially important given the proliferation of "free" cloud services in which the cloud provider earns its profit by mining the data entrusted to it by users and selling that data to advertisers or other third parties. While there is nothing inherently wrong with these ad-supported business models, users need to understand the nature of the data being collected and how it is used so that they may make an informed decision before accepting such a bargain. In some cases, consumers and small and medium

(October 23, 2012), *available at* http://www.microsoft.com/en-us/news/download/legal/10-23puttingpeoplefirst.pdf.

60. *See* INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — CODE OF PRACTICE FOR PII PROTECTION IN PUBLIC CLOUD ACTING AS PII PROCESSORS, ISO/IEC DIS 27018 (INT'L ORG. FOR STANDARDIZATION 2013), *available at* http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498.

sized businesses may decide not to hand over data to a free service if the nature of the data collected and how it is disclosed to third parties creates risk to reputation, economic interests, or personal privacy. Indeed, consumers increasingly are giving attention to how information provided to a cloud service can have consequences in other contexts; for example, concerns about employer use of prospective employees' social media accounts have led policymakers in the United States to consider legislation that would limit that use.[61] In an era in which users must consider the consequences of their digital "paper trails," honest disclosure from cloud providers as to their privacy and data use practices is essential.

### 3. Enabling and Protecting Cross-Border Data Flows

Being able to move data among multiple geographic areas allows cloud computing providers to pool IT resources and consolidate overheads and purchasing power. In turn, this results in significant cost and efficiency benefits for consumers, as well as the environmental benefits that flow from using fewer data centers.[62] Particularly important is the scale needed to make a viable cloud service available at the most accessible price point. While each new server employed in service of a public cloud carries notable cost reductions, there is an even greater cost reduction once at least 10,000 servers are employed in a public cloud.[63] From an operational standpoint, cloud computing providers move data between data centers in order to offer key services to customers, including 24-hour technical support and round-the-clock product development. Data transfer likewise is essential to data back-up and resiliency. As noted in a recent report by the Lloyd's insurance market, "The digital world is still susceptible to physical disasters such as flooding, earthquakes and hurricanes," and thus "geographic concentration" of data may increase risk of loss.[64] The

61. *See, e.g.*, *Employer Access to Social Media Usernames and Passwords 2013*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords-2013.aspx (last visited Sept. 23, 2013).

62. *See* Niels Soelberg, *The Economics of Cloud Computing for the EU Public Sector*, http://www.microsoft.com/eu/transforming-business/article/the-economics-of-cloud-computing-for-the-eu-public-sector.aspx (last visited Sept. 23, 2013).

63. FEDERICO ETRO, THE ECONOMIC IMPACT OF CLOUD COMPUTING ON BUSINESS CREATION, EMPLOYMENT AND OUTPUT IN EUROPE AN APPLICATION OF THE ENDOGENOUS MARKET STRUCTURES APPROACH TO A GPT INNOVATION (Feb. 2009).

64. LLOYD'S, DIGITAL RISKS - VIEWS OF A CHANGING RISK LANDSCAPE, LLOYD'S EMERGING RISKS TEAM REPORT (Oct. 2009), *available at* http://www.lloyds.com/~/

cloud provides a perfect vehicle for ensuring that critical information does not disappear forever as a result of natural or man-made disasters since cloud service by its nature does not concentrate the back-up of data in the same place; instead, it distributes back-ups across different parts of the world to maximize efficiency and continuity of the service, and cost savings to consumers.

Rules restricting the transfer of data and information across borders, however, do not accommodate the current realities of broadband-enabled computing. While not their intention, these rules limit the innovation and economic development otherwise made possible by the cloud, and often do not produce any corresponding benefit to consumer privacy. As the European Commission has recognized, "there is a general need to improve the current mechanisms for international transfers of data" in light of the vastly increased delivery of services over the Internet since the Data Protection Directive was adopted fifteen years ago.[65] The Directive as it now stands broadly restricts the transfer of personal data from within Europe to any country whose domestic laws do not provide a level of protection that the EU considers "adequate." In practice, only those countries that provide the same precise methods of protection as the EU, such as Argentina and Uruguay, have been deemed adequate.[66] In total, only seven countries have been deemed adequate, along with five microstates or dependent territories such as the Isle of Man.[67] Thus, in practice, the EU adequacy regime has placed broad constraints on the movement of data across borders, even where doing so compromises realization of cloud computing's benefits.

The "Safe Harbor" exception for the United States adopted by the EU, however, recognizes that while the U.S. does not employ the same precise methods of privacy protections as the EU, it is not necessary to deny the citizenry of an "adequate" country the benefits of cloud infrastructure found in major markets such as

media/lloyds/reports/emerging%20risk%20reports/digitalrisksreport_october2009v2.pdf.

65. *See A comprehensive approach to personal data protection in the European Union*, COM (2010) 609 final (Apr. 11, 2010), *available at* http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf.

66. *Commission decisions on the adequacy of the protection of personal data in third countries*, EUROPEAN COMMISSION JUSTICE, http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (last updated July 16, 2013).

67. *Id.*

the United States.[68] Instead, other mechanisms can be developed to enable the free but secure flow of data across borders. Under the Safe Harbor, companies in the U.S. can certify that they will import data from the EU only under conditions that conform to EU privacy laws.[69] Not all countries which limit data transfers to "adequate" countries, however, have adopted alternative compliance mechanisms such as the safe harbor framework adopted by the EU. Establishing these mechanisms in the many Latin American countries that have adopted EU-style data transfer restrictions could be key to the development of robust cloud computing services in Latin America.[70]

Regardless of the nature of an unduly strict cross-border data restriction—whether it is the result of an express prohibition on data export, a limitation based upon an "adequacy" requirement, or inconsistent laws across jurisdictions—the unintended consequence of putting a country fence around a local cloud is to depress investment, reduce trade, and deprive consumers and enterprises of the benefits of cloud computing and other innovations.

Alternatively, forcing a provider to store data locally in the jurisdiction that imposes restrictions on free data flows prevents the provider from being able to offer customers the cost and service benefits that stem from being able to move data to the most efficient storage place. There would also be an elimination of the potential energy efficiencies and environmental benefits of consolidating resources in fewer data centers.[71] In a nutshell, the desire for local data centers is in conflict with the efficiencies associated with the scale economics of cloud computing. To the extent that there is any short-term gain in forcing cloud providers to build

68. U.S. – E.U Safe Harbor Overview, EXPORT.GOV, http://export.gov/safeharbor/eu/eg_main_018476.asp (last updated July 1, 2013).

69. *Id.*

70. The European Commission (EC) recently published certain recommendations intended to improve the functioning of the Safe Harbor mechanism. While stakeholders have diverse views as to these recommendations, the EC recognized that "the Safe Harbor is an important component of the EU-US commercial relationship relied upon by companies on both sides of the Atlantic." In making its recommendations, the EC further recognized that any revocation of the Safe Harbor would be unwise, noting that it "would adversely affect the interests of member companies in the EU and in the US," and concluding instead that "the Safe Harbor rather be strengthened." *See* EUROPEAN COMMISSION JUSTICE, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL: REBUILDING TRUST IN EU-US DATA FLOWS 6 (Nov. 27, 2013), *available at* http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf.

71. *See* Soelberg, *supra* note 62.

local data centers as a condition to doing business, in the longer term such gains will be dwarfed by lost opportunities from the many cloud providers who simply choose not to make cloud services available in the country. Moreover, mandates to install local data centers produce little economic benefit within the country, as they rest upon the false assumption that physical data centers—as opposed to the services those data centers make possible—drive job growth in the cloud.[72]

### 4. Harmonization of Data Protection Rules and Interoperability

The cloud's defining feature is its lack of physical boundaries. This allows users in any country to create, access, and share data with others worldwide. Unfortunately, this lack of boundaries means that a cloud provider is potentially subject to the laws of hundreds of nations and thousands of jurisdictions.[73] Privacy and data security laws vary widely.[74] Some countries impose strict notice and consent requirements, while others have none.[75] Some countries limit the transfer of data to other countries, while others do not restrict data flow.[76] Some countries require companies to carefully guard personal information, while others require no such safeguards.[77]

Privacy laws and regulations have varied for decades. But the rise of cloud computing has magnified the problems caused by these inconsistencies. A truly global cloud provider must ensure that it is meeting the requirements of all privacy and data security laws, even if the laws conflict with one another. We need rules of the road that increasingly apply consistently in country after country and continent after continent. It would be unrealistic to expect every country to adopt identical data protection and privacy rules. But if countries made an effort to harmonize certain

72. *See* James Heaney, *Yahoo Aims to Expand Data Center in Lockport*, BUFFALO NEWS (April 4, 2011, 12:01 AM), http://www.buffalonews.com/article/20110404/CITYANDREGION/304049993 ("Data centers are not regarded as significant economic engines, however.").

73. *See* Juliette Garside, *How global laws protect your data*, THE GUARDIAN (Oct. 16, 2011, 7:01 PM), http://www.theguardian.com/cloud-technology/global-laws-protect-your-data.

74. *See* Constance Gustke, *Which countries are better at protecting privacy*, BBC (June 26, 2013), http://www.bbc.com/capital/story/20130625-your-private-data-is-showing.

75. *Id.*

76. *Id.*

77. *Id.*

requirements, they would reduce the uncertainty for cloud providers. Only through government-to-government collaboration can they create the consistency among regulatory frameworks that is necessary to make the cloud work. Governments could begin by working to develop rules that will facilitate data flows across national and regional borders. Alternatively, governments could work together to develop and agree upon shared principles for determining when a country has jurisdiction over data stored in the cloud.

It may prove most effective for governments over time to seek a multilateral framework on these issues in the form of treaties or similar international instruments. While this option undoubtedly would require significant diplomatic leadership and resources, it offers perhaps the best hope of addressing legitimate government needs in a coherent fashion while ensuring that business and consumer interests in privacy are met on a global scale.

A less formal option would be for countries to engage on a bilateral or regional basis in consultations and consensus building to better harmonize their respective data protection regimes and better resolve data access issues. Such engagement can increase awareness of the problems and pave the way for a longer-term, more formal solution. For example, in Asia, progress made on the ASEAN-Australia Development Cooperation Program on harmonizing e-commerce legal frameworks and the APEC Privacy Framework and Pathfinder Projects provides a solid platform for further development and addressing of the divergent jurisdictional approaches to technology policy. And the voluntary ISO 27001/27002 standards ensure information security at companies worldwide. Such multi-party, regional discussions offer an opportunity to boost cloud computing and expand its benefits on many levels across a region.

As Latin American nations adopt new data protection laws and regulations, they also should make interoperability a priority. As a starting point, countries should ensure that there is an interoperable framework within the region. For example, cloud computing enterprises should generally be able to expect that if they comply with Mexican rules and regulations on data privacy, they will not have to make significant changes to their practices in order to comply with Chilean rules, or vice versa. An interoperable, harmonized framework also could provide the region with a clearer and weightier voice in the global dialogue over data protection regulations and the cloud. The ultimate goal should be to

ensure that data protection rules in Latin American nations are interoperable with those of other regions, including in the U.S., EU and Asia. As noted, rigid "adequacy" determinations create needless complications to the data flows that make the cloud a reality.

### 5. Strengthening Laws Against Cybercrime

By preventing cybercrime, governments can help build consumer confidence in the cloud. When we say "cybercrime," we're referring to a variety of online criminal activities. The three general types of cybercrime that pose the biggest threat to the cloud are as follows: 1) crimes against individual citizens, such as attacks on children, 2) crimes against nations such as terrorism, and 3) economic crimes such as credit card fraud.[78]

Fighting cybercrime always has been a global issue, but cloud computing makes it more so. With a victim often in one jurisdiction, the datacenter or centers in other jurisdictions, and the perpetrator in yet another jurisdiction, there must be an effective mechanism for cooperation among law enforcement agencies in Latin America, the EU, the U.S., and elsewhere. There is a need for clear and consistent standards for production, retention and preservation of data in investigations that concern multiple jurisdictions; investment in technological know-how for local law enforcement; and cooperation in the establishment of international clearinghouses, through which data on cybercrimes is shared with a central point of global contact to evaluate trends and make connections that will help identify perpetrators.

In sum, by providing a consistent regulatory framework that protects privacy and instills customer confidence, the government can help promote national competitiveness through cloud computing.

## III. Challenges, Trends, and the Early Experience of Cloud Regulation

The cloud not only presents unprecedented opportunities; it also presents new privacy and data security questions for industry, regulators, and consumers. All stakeholders must identify

78. *See, e.g.*, Elinor Mills, *Cybercrime moves to the cloud*, CNET (June 30, 2012, 6:00 AM), http://news.cnet.com/8301-1009_3-57464177-83/cybercrime-moves-to-the-cloud/ (discussing how the cloud could be targeted by cyber criminals); *see also Top Threats to Cloud Computing V1.0*, Cloud Security Alliance (March 2010), *available at* https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

these challenges and determine the most effective way to address these questions while taking advantage of the cloud's full potential for local innovation and economic prosperity.

### *A. Cloud Computing Presents Important Privacy and Data Security Questions*

The need for thoughtful decision-making is especially pronounced in our era of "big data," which is the collection, management, and use of data on a massive scale. Even where individual items of information by themselves are relatively innocuous, in the aggregate these various bits of data can "begin to paint a portrait of a person's life."[79] In one particularly vivid example, the New York Times detailed how a large retailer was able to predict that a teenage girl was pregnant—and send her relevant coupons—even before her father knew, based simply on her purchasing history.[80] Online advertising networks have access to a much broader array of information. Researchers at Stanford University, for instance, found one advertising network that used a script to determine users' browsing histories and match the visited pages with a wide variety of interest segments, including such sensitive topics as credit repair and debt relief.[81]

Organizations moving to the cloud—be they businesses, government agencies, schools, or other institutions—have understandable concerns about the privacy and security of their data, the effect of regulatory compliance, and data usage policies of cloud providers. A recent survey conducted by the Cloud Security Alliance found that organizational users view information security as the leading constraint on cloud adoption.[82]

Individual users have similar concerns. They must be assured that their data is secure and safe from hackers, and that they can control who accesses their personal information. Establishing trust and confidence is necessary to promote access and

79. Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1141 (2002).

80. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

81. Jonathan R. Mayer & John C. Mitchell, *Third-Party Web Tracking: Policy and Technology* (2012), *available at* https://cyberlaw.stanford.edu/files/publication/files/trackingsurvey12.pdf; Jonathan Mayer, *Tracking the Trackers: To Catch a History Thief*, CIS (July 19, 2011, 4:20 AM), http://cyberlaw.stanford.edu/node/6695.

82. Joe McKendrick, *Cloud's Full Impact is Still About Three Years Away, Survey Predicts*, FORBES (Oct. 12, 2012), http://www.forbes.com/sites/joemckendrick/2012/10/03/clouds-full-impact-is-still-about-three-years-away-survey-predicts/.

encourage investment. For the cloud to truly succeed, consumers must feel just as comfortable storing their information on the cloud as they do when they store the information on their personal hard drives.

### *B. Regulatory Trends*

Argentina was a trendsetter in 2000 when it enacted the first comprehensive data protection and privacy rules in Latin America.[83] These regulations built consumer confidence in the Internet and helped the country's information technology sector thrive. But many of these regulations no longer apply to the cloud today. Unfortunately, some countries in the region have continued to adopt laws that limit the benefits of the cloud. Nations with laws based on models developed in the 1990s must modernize their data protection and privacy rules to build trust in the cloud and maintain national competitiveness. We live in a digital world that has radically changed over the past decade, and these "pre-cloud" laws do not adequately deal with privacy and security for the cloud age that is now a reality.

Consistent privacy and data protection regulations can establish a helpful baseline for all cloud providers. Balanced regulations could establish consumer trust in the cloud and help promote the growth of this remarkable technology. Rather than articulate specific regulatory requirements, we believe that it is more useful to discuss the two general characteristics of effective cloud regulations.

First, the regulations must allow data to flow freely across borders, in circumstances where there are assurances that the data importer will take steps to protect and secure personal data. Like the Internet on which it is based, the cloud is worldwide. Cloud-based services may cross dozens or hundreds of national borders, and on the way, dozens or hundreds of regulatory frameworks. This patchwork of regulations needs substantial updating.

Second, the regulations must protect privacy and ensure the cloud is secure from unauthorized access. As demonstrated above, trust is essential for the success of the cloud. Privacy and security are cited as the two main impediments to broader cloud adop-

83. *See generally* Maxim Gakh, *Argentina's Protection of Personal Data: Initiation and Response*, 2 I/S: J. L. & POL'Y FOR INFO. SOC'Y 781 (2006) (discussing Argentina's Data Protection Law and the effect its passage had on other countries).

tion.[84] A safe and open cloud is a cloud that is protected from hackers and thieves and that also serves as a reservoir of information that can serve all people with affordable, continuous services accessible from always-connected devices.

Governments wisely have begun to consider proposals that would protect consumer privacy in the cloud through an outcome-oriented regime. For example, the European Commission suggested that an "accountability" principle be expressly included in the EU data protection regime.[85] Under an accountability-based regime, data protection standards and requirements are enshrined in law, but individual organizations have much of the responsibility to determine how best to meet those standards in practice. It is important, however, that the benefit of an accountability approach not be squandered by simply imposing a requirement that organizations be accountable on top of the EU's existing prescriptive rules. Rather, accountability should be used instead of prescriptive rules, a point that the United Kingdom Information Commissioner made earlier this year when he opposed aspects of the proposed EU data protection rules.[86]

In that same vein, the U.S. Department of Commerce's recommended legislation would create a safe harbor from government enforcement actions for companies that adhere to appropriate voluntary, enforceable codes of conduct developed through multi-stakeholder processes. The Department of Commerce correctly emphasized that this flexible, safe harbor approach would not diminish protections for consumers, noting that "[f]ailing to comply with the voluntary, enforceable code's provisions could lead to an enforcement action by the FTC or a State Attorney General."

### *C. Microsoft's Approach*

Regulations alone will not build the necessary level of consumer trust in the cloud. Industry must have an ongoing dialogue with customers about cloud privacy. Microsoft is committed to

84. WORLD ECONOMIC FORUM, EXPLORING THE FUTURE OF CLOUD COMPUTING: RIDING THE NEXT WAVE OF TECHNOLOGY-DRIVEN TRANSFORMATION (2010), *available at* http://www.weforum.org/pdf/ip/ittc/Exploring-the-future-of-cloud-computing.pdf.

85. *Data Protection Accountability: The Essential Elements*, THE CENTRE FOR INFORMATION POLICY LEADERSHIP (Oct. 2009), *available at* http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf.

86. Liat Clark, *ICO Commissioner Slams EU Data Protection Directive*, WIRED UK (Feb. 7, 2013), http://www.wired.co.uk/news/archive/2013-02/07/ico-against-eu-data-protection ("We want it defined in terms of outcomes rather than regulatory process.").

playing a proactive and responsible role in this area. We firmly believe that privacy practices in the cloud will benefit from communications and services that inform consumers and compare offerings. By way of analogy, in the automotive industry, this sort of dialogue has been successful at driving industry to innovate in the area of safety—through government initiatives to inform consumers as well as consumer magazines and websites that rate cars based in part on safety standards and consumer input. A similar dialogue in the cloud computing context could facilitate industry responsiveness to privacy needs.

Microsoft, for example, obtains customer feedback through a variety of means, including usability tests, surveys, focus groups and other types of field research. Microsoft also created the Customer Experience Improvement Program (CEIP), through which customers may voluntarily share information online about how they use Microsoft programs and report any problems may encounter. This information helps Microsoft to innovate and improve the overall user experience, including with respect to the privacy and security of customers, which Microsoft is committed to protecting.

What Microsoft has learned from this feedback, among other things, is that customers want to better understand what data is being collected and how it is being used. In response, we have worked hard to provide clear and easy-to-understand information on our privacy and security practices. For example, Microsoft created the Office 365 Trust Center to provide an industry-leading level of transparency about data privacy and security practices. The Trust Center provides customers and other stakeholders with clear, easy-to-understand explanations of what Microsoft does with data in the cloud—including how it is collected, the circumstances under which it can be accessed, where the data flows, and how the customer can receive additional security, privacy and audit information.[87] The Trust Center is unique in the industry and has made Microsoft the leader in transparency in the cloud. In contrast to some cloud providers that are not fully transparent about their data use practices, Microsoft makes clear promises that it will use an enterprise customer's data *only* to provide the services requested by the customer, and not to benefit Microsoft commercially.

87. *Microsoft Office 365 Trust Center*, MICROSOFT CORP., http://office.microsoft.com/en-us/business/office-365-trust-center-cloud-computing-security-FX103030390.aspx (last visited Nov. 24, 2013).

When Microsoft is subpoenaed or legally mandated by governments to produce customers' information, Microsoft's position is clear: Microsoft believes that our customers should control their own information to the extent possible. Accordingly, if a governmental entity approaches Microsoft directly for information hosted on behalf of our Office 365 customers, for example, Microsoft will try in the first instance to redirect the entity to the customer to afford the customer the opportunity to determine how to respond. If Microsoft is nonetheless required to respond to the demand, Microsoft will only provide information belonging to its Office 365 customers when Microsoft is legally required to do so. Microsoft will limit the production to only that information which Microsoft is required to disclose, using reasonable efforts to notify the customer in advance of any production unless Microsoft is legally prohibited from doing so.[88] As stated by Microsoft General Counsel Brad Smith, "in no event will Microsoft provide governments with direct or unfettered access to customer data or encryption keys. Microsoft only pulls and then provides the specific data mandated by the relevant legal demand."[89]

Moreover, in light of recent allegations regarding surveillance of customer data by some governments, Microsoft is taking various preventive steps. Such steps include, for example, strengthening encryption across Microsoft networks and services (noting that customer data in Office 365 and Outlook.com already benefits from encryption when traveling between customers and Microsoft), and enhancing the transparency of Microsoft's software code (this will facilitate reassurances that Microsoft does not engineer back doors in Microsoft products which governments could surreptitiously exploit to access private customer data). At the same time, Microsoft is joining together with other companies across our industry such as AOL, Apple, Facebook, Google, LinkedIn, Twitter and Yahoo to call for reforms of government surveillance that will require government adherence to specific principles with respect to surveillance.[90]

On top of transparency, it is clear that consumers also want

88. How We Use Your Data, *Microsoft Office 365 Trust Center*, MICROSOFT CORP., http://www.microsoft.com/online/legal/v2/?docid=23 (last visited Nov. 24, 2013).

89. Brad Smith, *Responding to Government Legal Demands for Customer Data*, MICROSOFT ON THE ISSUES, (July 16, 2013), http://blogs.technet.com/b/microsoft_on_the_issues/archive/2013/08/30/standing-together-for-greater-transparency.aspx.

90. Brad Smith, *Protecting Customer Data from Government Snooping*, THE OFFICIAL MICROSOFT BLOG, (Dec. 4, 2013), http://blogs.technet.com/b/microsoft_blog/archive/2013/12/04/protecting-customer-data-from-government-snooping.aspx.

choice and control over how their data is used—particularly by commercial third parties. Again, we are working hard to be responsive. Internet Explorer provides "Tracking Protection." On today's Internet, websites increasingly pull in content, such as images and text, from third party sites. Although this is a common feature of modern web design that enables online providers to enhance their websites and services, users sometimes are not aware that they can be tracked across the web by third parties through content on the pages. Specifically, users will be able to create Tracking Protection Lists that allow users to limit the sharing of their data with specified sites, or categories of sites. Users may include whatever sites they desire in these lists, and in the future, we expect people will be able to choose Tracking Protection Lists that are created by all kinds of companies and organizations—from privacy advocates to security firms to advertising trade groups. Importantly, Tracking Protection puts users in control without employing intrusive mechanisms that detract from the online experience, such as interrupting users potentially hundreds of times a day to request affirmative consent every time a cookie is deployed.[91] The European Privacy Association recently praised Tracking Protection as contributing to "the creation of an online market more focused on consumers' needs and attentive to their privacy concerns."[92]

Microsoft gives consumers similar levels of choice and control across our technologies and services. Windows Phone 8, for instance, includes a "geo-location" feature that enables consumers to take advantage of the increasing array of location-based applications and services on the market. However, no application can gain access to that location information unless the consumer has provided affirmative consent. Applications that use consumers' locations also are required to allow users to turn off that access at a later time—and consumers have the option of turning off location access for all applications.

Microsoft also provides enterprise customers with sophisticated tools for managing the use of sensitive information within their own organizations—using innovations such as Windows 8 BitLocker and BitLocker To Go, which encrypt data on PCs and

91. More information on our Tracking Protection feature is available at *IE9 and Privacy: Introducing Tracking Protection*, IEBLOG (Dec. 7, 2010, 1:10 PM), http://bit.ly/ietpl.

92. European Privacy Association, *Protection list: on the Right Track*, EPA NEWS (Jan. 21, 2011), http://www.europeanprivacyassociation.eu/agenda_news.php?function=read&id=36.

portable USB devices and thereby prevent access to an organization's sensitive data if an employee device is lost or stolen.[93]

In short, Microsoft is committed to maintaining leadership in the industry on privacy in the cloud. Why? In addition to the company's firmly held convictions about privacy and security, Microsoft's business model—which is primarily built on generating revenue from the sale of innovative software and services—drives Microsoft to protect user privacy. In contrast, some cloud providers generate revenue almost exclusively by mining consumer data found in emails, online searches, etc., to serve such companies' advertising clients (as the saying goes, "if you get a product for free, *you* are the product").[94] This leads to very different incentives and approaches on privacy. Because of Microsoft's business model, Microsoft views privacy as having tremendous commercial value to users, and we believe that Microsoft and others in industry should compete to provide the best privacy protections available.

Of course, while competitive offerings will produce many benefits in the privacy arena, industry collaboration and self-regulation are also critical to promote online privacy—a point that the European Commission recognizes in its Digital Agenda for Europe.[95] That is why Microsoft shares with partners and competitors the privacy guidelines Microsoft follows when developing software and online services.[96] Since Microsoft first made these guidelines available in 2006, they have made significant contributions to the leading professional privacy certification in the IT sector (the Certified Information Privacy Professional for IT, or CIPP/IT) and have helped to shape international privacy standards.

We see a number of opportunities for further dialogue with

93. For more information on security tools provided in Windows 8, *see* http://www.microsoft.com/security/pc-security/windows8.aspx. In addition, Microsoft certifies its online services to the ISO 27000 series of security standards, which among other things establish guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization.

94. Bryan Cunningham, *Google's data mining raises questions of national security*, THE GUARDIAN (Oct. 15, 2012, 11:40 AM), http://www.theguardian.com/commentisfree/2012/oct/15/google-data-mining-national-security ("The revenue generated by combining and monetising such data—by mining the mosaic—is the reason "free" cloud services can afford to be free.").

95. *See* A DIGITAL AGENDA FOR EUROPE, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS §2.3 (TRUST AND SECURITY) (2010).

96. *Privacy Guidelines for Developing Software Products and Services Version 3.1*, MICROSOFT CORP. (2006) *available at* http://go.microsoft.com/?linkid=9746120.

industry partners on self-regulation. For example, as geo-location data is increasingly being collected and used to provide a range of services to users, several organizations are leading efforts to create codes of conduct to help assuage emerging concerns of regulators around the collection and use of such data. Microsoft will continue to actively participate in and support efforts to help create coherent, privacy protecting practices across the industry.

## IV. CONCLUSION

Cloud computing can uplift economies by creating jobs and driving innovation, foster greater social inclusion, and create higher living standards because it is available at a price that is itself very inclusive. To bring about the economic growth and societal benefits that cloud computing offers, governments and industry must work together, just as they did in fostering past eras of innovation-driven growth. Microsoft is committed to doing its part, both through market-leading privacy and security practices, and through support of regulatory frameworks and industry self-regulation. Already in Latin America, the U.S., and other jurisdictions, governments have begun to map out necessary measures in consultation with a broad array of stakeholder groups. We encourage governments to revisit regulatory frameworks as needed to better empower their cloud platforms so that the latest features and services may be offered to local citizens at an affordable price, and so that local innovators may share their inventions with the world. Looking back someday, it will be said that those data protection frameworks that facilitated cloud computing were the ones which best served a country's aspirations for national competitiveness.

* * *