AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

CLOUD COMPUTING: AN OVERVIEW OF THE TECHNOLOGY AND THE ISSUES FACING AMERICAN INNOVATORS

HEARING

BEFORE THE

SUBCOMMITTEE ON
INTELLECTUAL PROPERTY,
COMPETITION, AND THE INTERNET

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

JULY 25, 2012

Serial No. 112–122

Printed for the use of the Committee on the Judiciary



Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE

75–311 PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

LAMAR SMITH, Texas, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
STEVE CHABOT, Ohio
DARRELL E. ISSA, California
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TIM GRIFFIN, Arkansas
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
DENNIS ROSS, Florida
SANDY ADAMS, Florida
BEN QUAYLE, Arizona
MARK AMODEI, Nevada

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO R. PIERLUISI, Puerto Rico
MIKE QUIGLEY, Illinois
JUDY CHU, California
TED DEUTCH, Florida
LINDA T. SÁNCHEZ, California
JARED POLIS, Colorado

RICHARD HERTLING, *Staff Director and Chief Counsel*
PERRY APELBAUM, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON INTELLECTUAL PROPERTY, COMPETITION, AND THE INTERNET

BOB GOODLATTE, Virginia, *Chairman*
BEN QUAYLE, Arizona, *Vice-Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
STEVE CHABOT, Ohio
DARRELL E. ISSA, California
MIKE PENCE, Indiana
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TIM GRIFFIN, Arkansas
TOM MARINO, Pennsylvania
SANDY ADAMS, Florida
MARK AMODEI, Nevada

MELVIN L. WATT, North Carolina
JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
JUDY CHU, California
TED DEUTCH, Florida
LINDA T. SÁNCHEZ, California
JERROLD NADLER, New York
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
HENRY C. "HANK" JOHNSON, JR., Georgia

BLAINE MERRITT, *Chief Counsel*
STEPHANIE MOORE, *Minority Counsel*

CONTENTS

JULY 25, 2012

Page

OPENING STATEMENTS

The Honorable Bob Goodlatte, a Representative in Congress from the State of Virginia, and Chairman, Subcommittee on Intellectual Property, Competition, and the Internet 1

The Honorable Lamar Smith, a Representative in Congress from the State of Texas, and Chairman, Committee on the Judiciary 3

WITNESSES

Robert W. Holleyman, II, President and Chief Executive Officer, Business Software Alliance (BSA)
Oral Testimony 6
Prepared Statement 8

Justin Freeman, Corporate Counsel, Rackspace US, Inc.
Oral Testimony 15
Prepared Statement 17

Daniel Chenok, Executive Director, Center for the Business of Government, International Business Machines Corporation (IBM)
Oral Testimony 27
Prepared Statement 28

Daniel Castro, Senior Analyst, Information Technology and Innovation Foundation (ITIF)
Oral Testimony 33
Prepared Statement 35

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Prepared Statement of the Honorable Melvin L. Watt, a Representative in Congress from the State of North Carolina, and Ranking Member, Subcommittee on Intellectual Property, Competition, and the Internet 2

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Letter from Robert W. Holleyman, II, President & Chief Executive Officer, Business Software Alliance (BSA) 64

Supplemental Material submitted by Robert W. Holleyman, II, President & Chief Executive Officer, Business Software Alliance (BSA) 67

Report by TechAmerica Foundation 114

Prepared Statement of William Weber, General Counsel, Cbeyond, Inc. 149

OFFICIAL HEARING RECORD

MATERIAL SUBMITTED FOR THE HEARING RECORD BUT NOT REPRINTED

111th Congress hearing entitled ECPA Reform and the Revolution in Cloud Computing, September 23, 2010, Subcommittee on the Constitution, Civil Rights, and Civil Liberties, Committee on the Judiciary, submitted by the Honorable Melvin L. Watt, a Representative in Congress from the State of North Carolina, and Ranking Member, Subcommittee on Intellectual Property, Competition, and the Internet. The hearing is not reprinted in this record but is available at the Committee and can be accessed at:

http://judiciary.house.gov/hearings/printers/111th/111-149—58409.PDF.

CLOUD COMPUTING: AN OVERVIEW OF THE TECHNOLOGY AND THE ISSUES FACING AMERICAN INNOVATORS

WEDNESDAY, JULY 25, 2012

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INTELLECTUAL PROPERTY,
COMPETITION, AND THE INTERNET,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to call, at 12:10 p.m., in room 2141, Rayburn Office Building, the Honorable Bob Goodlatte (Chairman of the Subcommittee) presiding.

Present: Representatives Goodlatte, Smith, Marino, Watt, Nadler, and Lofgren.

Staff present: (Majority) Vishal Amin, Counsel; Olivia Lee, Clerk; and (Minority) Stephanie Moore, Subcommittee Chief Counsel.

Mr. GOODLATTE. Good afternoon. The Subcommittee of Intellectual Property, Competition, and the Internet will come to order. And I will recognize myself for an opening statement.

Today we are holding a hearing on cloud computing. Cloud computing represents a fundamental shift in the delivery of services, software, and data storage. The move toward cloud services helps lower the barriers to entry and democratizes access to technology for small- and medium-sized businesses.

Companies no longer need to purchase or build server farms or have an IT team to deal with security issues and hardware malfunctions. The cloud brings together reduced costs, device and location independence, reliability, scalability, security, and performance.

But with new technology come new issues that deal with security, privacy, and market access. As more software becomes cloud or Internet-based, cybersecurity and privacy issues become intertwined.

To set the stage for today's hearing, we have witnesses that can speak to the key service areas of cloud computing. These include infrastructure, platform, and software. Infrastructure as a service refers to storage where companies offer dedicated or share servers to customers to store their information. Platform as a service means that a company is delivering an operating system that allows others to build new apps on top of their system. The third flavor of cloud refers to software as a service. Here the software is installed in the cloud, eliminating the need for physical copies of soft-

ware. Updates occur seamlessly, and customers access the software through the Internet.

But apart from the overall technology, there are issues that companies in this industry are concerned about, and there are issues that our customers are concerned about. In the market access arena, cloud companies need to be able to operate globally, and restrictions placed on cloud providers in particular countries can effectively limit market access and prevent services from being delivered to and adopted by consumers.

There are also issues dealing with international operability. As cloud computing services take hold, it is important for there to be clear rules of the road when it comes to industry standards and international rules. Cloud companies and customers also have a strong interest in ensuring that the privacy and security of the data stored and used on their systems is secure.

For consumers, it means they want to know how their personal information is being used and protected. For companies, the concern is on security, ensuring that company trade secrets and business information is adequately protected and easily accessible in the cloud.

I look forward to hearing from all of our witnesses on these and other issues that they are seeing, and also engage in a discussion on the issues that cloud computing faces going forward. We need to ensure that as this new American technology sector grows, it is able to compete on a level playing field abroad and to promote U.S. innovation technology and jobs.

And with that, it is my pleasure to recognize the Ranking Member, the gentleman from North Carolina, Mr. Watt.

Mr. WATT. Thank you, Mr. Chairman, and I think the Chairman has sufficiently outlined the range of issues that are, I think, important to this hearing. It is an important hearing about things in the cloud, which some people say that is where I always am. So I want to figure out what is going on up there.

I think I will just submit my statement for the record. I will have some questions about how we can incentivize competition in the cloud. But except for that, I think the Chairman has outlined the issues. So I will submit my statement for the record.

I know we have got a very short time window that we are operating in, and I think hearing the witnesses is a lot more important than hearing me. So I will yield back.

Mr. GOODLATTE. I thank the gentleman, and without objection, his entire statement will be made a part of the record.

[The prepared statement of Mr. Watt follows:]

Prepared Statement of the Honorable Melvin L. Watt, a Representative in Congress from the State of North Carolina, and Ranking Member, Subcommittee on Intellectual Property, Competition, and the Internet

Thank you, Mr. Goodlatte.

I will be brief. This hearing promises to cover a full range of issues involved with cloud computing. For many consumers, migration to the cloud has been driven by fast broadband connections, low-cost mobile devices and a mobile population that expects access to data and applications anywhere and anytime. This generation has become accustomed to the luxury of never having to delete an e-mail or document because of the "unlimited" and safe storage capabilities cloud computing affords. Organizations, including start-ups, are also embracing cloud computing because of the

flexibility and agility it provides. A business, for example, can scale up or down its information technology "IT" usage according to demand with no long term commitments and no high imbedded costs.

These extraordinary benefits to companies and individuals alike also come with increased concerns about reliability, security and privacy. The power outages earlier this month at Amazon's Web Services datacenter in North Virginia due to fierce thunderstorms throughout the Mid-Atlantic region of the U.S. raise lingering concerns about the reliability of cloud services. Two weeks later, the District's Metro subway system experienced a mysterious software failure that has been widely subject to speculation that its data center was hacked. As the migration to the cloud continues, companies must take care to ensure the security of their systems on several levels.

There are multiple layers of privacy concerns as well. Although I am sympathetic to the barriers companies are facing internationally due to other countries' perceptions of our privacy laws, I am more concerned with the consumer's right to privacy within the cloud. While I continue to believe that consumer privacy is paramount, the cloud offers new and innovative ways for the technologically savvy criminal to exploit the cloud for nefarious purposes. The "Backpage" prostitution scandal with Craigslist is just one example. The cloud must develop with caution to ensure that illegality does not flourish within the cloud, and Congress should update the Electronic Communications Protection Act (ECPA) to provide clear guidance on when and how law enforcement is entitled to access otherwise private data and communications.

Finally, one area that I do not think has been given enough attention is competition in the cloud computing industry. Although news accounts suggest that competition is currently robust, there are concerns that it may be changing. I am interested in hearing more in this area—how we ensure continued competition and lower costs to businesses and consumers.

With that, Mr. Chairman, I yield back.

Mr. GOODLATTE. And it is now my pleasure to recognize the Chairman of the Judiciary Committee, the gentleman from Texas, Mr. Smith.

Mr. SMITH. Thank you, Mr. Chairman. I just want to point out to those who are present that I believe this is the first time this Subcommittee or any Committee has had a hearing on this particular subject. And I think that, Mr. Chairman, that is to your credit. This is an important subject and an important area of tech that is going to do nothing but increase in the future.

I have a short opening statement, and then we will get on to the panelists.

America's economic success has been built on innovation. Cloud computing can transform everything from business operations, data storage, and analysis to the delivery of software and services to businesses and consumers alike. The cloud industry is growing rapidly. Wall Street Journal reported that technology cloud services worldwide had $16 billion in revenue in 2009, and cloud service revenue is expected to double this year and hit $73 billion by 2015.

Because cloud providers can offer more robust data services at a lower cost than would be possible for a company to replicate for itself, the move to the cloud will help companies reduce information technology costs and add to their technical capabilities.

But as these new technologies and products develop, it is clear that certain foreign governments have taken steps to disadvantage American cloud companies by imposing barriers to market access. Some of the barriers include restrictive regulations or policies that

mandate the use of certain technologies or require a cloud service to be placed in country as a condition of doing business.

Cloud computing relies on the seamless flow of data across borders and international interoperability. Unfortunately, some countries have adopted rules that limit the specific types of data that can leave their borders, and have put in place restrictive regulatory frameworks.

Some countries also have spread deliberate misinformation about U.S. laws, like the PATRIOT Act, saying that it negatively affects the security and privacy protections that U.S. cloud providers offer compared to European providers. These actions hurt the competitiveness of American companies and cost Americans jobs.

Today's witness panel represents a range of cloud services, and I am pleased that Rackspace is here today. They are a San Antonio, Texas-based company that has operations throughout the world. Founded in the late 1990's, Rackspace now has nearly half of the Fortune 100 as clients. They provide cloud computing services for computing, cloud files for storage, and cloud applications for e-mail collaboration and file backups. They also manage web-based IT systems for small-, medium-, and large-sized business, and offers scalable services depending on its customers' needs.

Though the technology of cloud computing is new, the issues are not. As the U.S. government develops domestic policies and our policies with our international trading partners, we need to ensure that American innovators are treated fairly.

Thank you, Mr. Chairman, and I will yield back.

Mr. GOODLATTE. I thank the Chairman.

Mr. WATT. Mr. Chairman?

Mr. GOODLATTE. The gentleman from North Carolina is recognized.

Mr. WATT. I just wanted to make one minor correction to what Chairman Smith said. There was a hearing on Electronic Communications Protection Act reform and cloud computing. It was done September 23, 2010, by Jerry Nadler's Subcommittee, the Subcommittee on the Constitution of this Committee. And so technically we have not had a hearing specifically on the cloud, but this was an aspect of it, so I will submit the record of that hearing with unanimous consent just so it will all be part of the record.

Mr. GOODLATTE. Without objection, the noting of the previous hearing in the Constitution Subcommittee will be duly noted.*

Without objection, other Members' opening statements will be made a part of the record.

Mr. SMITH. I said this was the first time this Subcommittee had had such a hearing on this——

Mr. WATT. Or any Committee. That is where you went awry. But I acknowledge that technically you were probably——

Mr. SMITH. Let us not waste any more time on that.

Mr. GOODLATTE. We will be pleased to begin the first hearing on cloud computing of this Subcommittee by hearing from our witnesses. We have a very distinguished panel of witnesses today.

---

*The hearing submitted by Mr. Watt, entitled ECPA Reform and the Revolution in Cloud Computing, is not reprinted in this hearing record but is available at the Committee and can be accessed at http://judiciary.house.gov/hearings/printers/111th/111-149—58409.PDF.

Each of the witnesses' written statements will be entered into the record in its entirety, so I ask that each witness summarize his testimony in 5 minutes or less. To help you stay within that time, there is a timing light on your table. When the light switches from green to yellow, you will have 1 minute to conclude your testimony. When the light turns red, it signals that the witness' 5 minutes have expired.

And as is the custom of this Subcommittee, before I introduce the witnesses, I would like them to stand and be sworn.

[Witnesses sworn.]

Mr. GOODLATTE. Thank you very much, and please be seated.

Our first witness is known to and a good friend of many Members of the Judiciary Committee, Mr. Robert Holleyman. He serves as the President and CEO of the Business Software Alliance. He has headed BSA since 1990, expanding their operations to more than 80 countries and launched 13 foreign offices in addition to their D.C. headquarters.

Mr. Holleyman has been named one of the 50 most influential people in the intellectual property world by the international magazine Managing IP. He was also named by the Washington Post as one of the key players in the U.S. government's cybersecurity efforts for his work on behalf of industry on national cybersecurity policy.

Before joining BSA, Mr. Holleyman served as counsel in the U.S. Senate and as an attorney with a leading law firm in Houston, Texas. He earned his Bachelor of Arts degree at Trinity University in San Antonio, Texas, and his Juris Doctor from Louisiana State University Law Center in Baton Rouge. He also completed the Executive Management Program at the Stamford Graduate School of Business.

And it is my pleasure to turn to the Chairman of the Committee on the Judiciary, Mr. Smith, to recognize and introduce our second witness.

Mr. SMITH. Thank you again, Mr. Chairman. I am happy to introduce Mr. Justin Freeman, Corporate Counsel of Rackspace Hosting based in San Antonio.

Rackspace, founded in 1998, has grown into a multinational company with operations spanning the globe. They provide cloud computing services and manage web-based IT systems for businesses of all sizes.

Mr. Freeman is part of Rackspace's legal team and deals primarily with the rapidly expanding field of cloud computing. He represents Rackspace in technically complex enterprise transaction agreements, leads product review and development efforts, and directs public policy matters with a focus on cloud computing security and privacy issues. He has an extensive technical background, including specialization in network security systems and patient care, critical healthcare IT systems.

Mr. Freeman received his law degree from Southern Methodist University School of Law and his undergraduate degree from the University of Texas at Austin. We are pleased he is here today to talk more about this important and growing sector of our tech economy. Welcome, Mr. Freeman.

Mr. GOODLATTE. Mr. Freeman, welcome. And, Mr. Chenok, welcome. Our fourth witness is—third witness is Mr. Dan Chenok, Executive Director of the IBM Center for the Business of Government. The center connects public management research with practice, helping executives improve the effectiveness of government with practical ideas, which has included several center reports that address cloud computing.

Mr. Chenok also serves as the Chair of the Federal Information Security and Advisory Board, which has explored numerous issues where security and privacy intersect with cloud computing.

Before joining IBM, he was a Senior Vice President for Civilian Operations with Pragmatics. He also served in the Office of Management and Budget, in the Executive Office of the President, as the Branch Chief for Information Policy and Technology. Mr. Chenok left the government in 2003.

He received his Master of Public Policy from Harvard University John F. Kennedy School of Government and his B.A. from Columbia University.

Our fourth witness is Mr. Daniel Castro, Senior Analyst at the Information Technology and Innovation Foundation, ITIF. Mr. Castro specializes in IT policy, including issues relating to data privacy, e-commerce, e-government, and information security and accessibility. Before joining ITIF, Mr. Castro worked as an IT analyst at the Government Accountability Office, GAO, and was a Visiting Scientist at the Software Engineering Institute in Pittsburgh, Pennsylvania.

Mr. Castro received his B.S. in Foreign Service from Georgetown University and an M.S. in Information Security Technology and Management from Carnegie Mellon University.

Welcome to you all, and we will begin with Mr. Holleyman.

TESTIMONY OF ROBERT W. HOLLEYMAN, II, PRESIDENT AND CHIEF EXECUTIVE OFFICER, BUSINESS SOFTWARE ALLIANCE (BSA)

Mr. HOLLEYMAN. Chairman Goodlatte, Ranking Member Watt, Chairman Smith, thanks to companies like those who are in the Business Software Alliance and sitting here at this table, America is the top player in cloud computing. But we better watch out. Other countries are doing everything they can to knock us off the block.

They have seen the forecasts that we all have seen. Public IT cloud revenue, which exceeded $28 billion last year, will grow to more than $73 billion by 2015. But the big thing that is happening is the innovation enabled by the cloud. A recent study found that cloud-driven innovation across all sectors will generate more than a trillion dollars in revenue and millions of jobs in the years ahead.

Because the stakes are so high, and because of U.S. cloud companies' early leadership, some countries are taking policy steps to shut us out of their markets. The stakes of this are enormous, and if we want to get things right and to continue leading in the cloud, there is an urgent need for Congress and the Administration to forge an open and competitive global landscape.

I would like to cover three things today: first, the scope of the problem, second, the mix of public policies that are needed to ad-

dress it, and, third, some specific things that this Committee can do.

The problem before us is unfolding around the world. As was indicated in my introduction, BSA has 13 foreign offices, and we have done a lot of on-the-ground work and two ground-breaking studies about the cloud. One is a global "Cloud Scorecard" that looks at 80 percent of the global ICT market and ranks the competitiveness and a host of factors that affect the U.S. and other countries, and the ability of companies to succeed in the cloud. And the second is "Lockout," which is a report about a new wave of IT barriers that are being erected internationally.

Our research shows that governments in many countries are doing things to carve the cloud up into country-sized pieces so that local players can dominate their own backyards without competition. For example, in the name of privacy and security, we are seeing some countries require data to be hosted inside their borders, even non-sensitive commercial information. You would have to build a local data center to do business in some of these countries, and that could put a prohibitive burden on international cloud players.

Some countries are even adopting rules that would explicitly prevent the transfer of personal information outside their borders. Now these are bad signs for the global economy, but especially for America since we are so heavily dependent on selling products and services overseas.

It is critical for Congress and the Administration to show the world a better mix of cloud policies. And we can do that by getting three things right. First, we need to ensure that privacy and security rules protect consumers while also encouraging robust digital commerce. Second, we need to promote a free trade agenda that ensures that data can flow across borders. And third, we need to promote innovation in the cloud the same way we promote it everywhere else. That means protecting innovators' rights when they bring new products to market, and it means stopping all forms of cybercrime and theft.

This Committee has an important role to play in this issue. For example, there is a myth that cloud computing puts an end to software piracy. In reality, piracy is evolving. This Committee can ensure that we have tools to vigorously enforce laws against IP theft no matter where that technology or how that technology is used. Secondly, this Committee can take a lead role in reforming the Electronic Communications Privacy Act, ECPA. In the cloud era, digital files should be subject to the same laws and protections as paper files. And finally, we need to dispel myths about the PATRIOT Act. Foreign governments are scaring customers away from U.S. cloud services by portraying our law as unusually invasive. The fact is every government has authority to access data to protect national security, and everyone needs to understand that.

We look forward to discussing these issues with you and to working with the Committee. The future of the cloud computing industry and American leadership depends on your work. Thank you.

[The prepared statement of Mr. Holleyman follows:]



U.S. House of Representatives

Committee on the Judiciary

Subcommittee on Intellectual Property, Competition, and the Internet

Hearing on:
Cloud Computing:
An Overview of the Technology and the Issues Facing American Innovators

Testimony of Robert W. Holleyman II
President & CEO, Business Software Alliance

Wednesday, July 25, 2012

Chairman Goodlatte and Ranking Member Watt, thank you for holding this hearing today and for inviting me to testify. My name is Robert Holleyman. I am the president and CEO of the Business Software Alliance (BSA). BSA is an association of the world's leading software and hardware companies. BSA's members create approximately 90 percent of the office productivity software in use in the United States and around world.[1]

Increasingly that software is offered through "the cloud" – a model that enables flexible, on-demand access over the Internet. BSA member companies are early leaders in cloud computing technology, and they are leaders in the global cloud computing market as a result.

Leadership in the cloud is not assured, however. Countries around the world desperately hope to copy the model of technology-driven economic growth that powers the US economy. Far too often they would do so by throwing up protectionist barriers aimed to hurt international cloud providers and by adopting policies that would chop the cloud into country-sized pieces. Such policies would make it difficult for data to flow across international borders and to power the cloud. And such policies would come at the expense of a truly global cloud economy. Cloud computing technology won't scale to its full potential behind a series of walls. Countries need to adopt more harmonized policies – policies that will both promote user trust and help spur economic growth.

The importance of such policies points to the vital need for Congress and the United States to lead in the cloud. Toward that goal, BSA has outlined a seven-element "policy blueprint" for maximizing the economic opportunity that cloud computing presents. Following this blueprint is important internationally to ensure the cloud operates on a global scale. Closer to home, it also is vital that the United States follow these policies and avoid protectionist measures of our own. Doing otherwise would both undermine the global cloud and give cover to other countries that would do the same. Several of those elements – including key data privacy and cybercrime laws and intellectual property protections – fall under the jurisdiction of this Committee.

What Is Cloud Computing?

Cloud computing is not any one thing. It is a mix of software-enabled resources and services that can be delivered to the user on an "as needed" basis. Technically speaking, the National Institute of Standards and Technology's definition provides a widely accepted foundation:

---

[1] *The Business Software Alliance (www.bsa.org) is the leading global advocate for the software industry. It is an association of more than 70 world-class companies that invest billions of dollars annually to create software solutions that spork the economy ond improve modern life. Through internationol government relations, intellectual property enforcement and educational activities, BSA expands the horizons of the digital world and builds trust and confidence in the new technologies driving it forward.*

BSA's members include: Adobe, Apple, Autodesk, AVEVA, AVG, Bentley Systems, CA Technologies, CNC/Mastercam, Intel, Intuit, McAfee, Microsoft, Minitab, Progress Software, PTC, Quest Software, Rosetta Stone, Siemens PLM, Sybase, Symantec, and The MathWorks.

> "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

For individual consumers, cloud computing may most easily be understood as it is consumed: through the online services that enable users to create, manage, and store documents, spreadsheets, photos or other digital content so that they can be accessed from any computer over the Internet. But that is just the beginning. Cloud computing enables transformative possibilities for businesses as well.

The economic and social benefits inherent in cloud computing are important for enterprises of all sizes, for governments and for consumers. Cloud computing levels the playing field for access to technology. It allows single customers to enjoy the benefits that have long been enjoyed by major users. It opens the door to tremendous gains in efficiency, productivity and competitiveness for businesses in the global marketplace. For governments, cloud computing presents a two-fold opportunity: the chance to improve productivity and citizen engagement through IT procurements as well as the benefit of encouraging economic growth, sustainable job creation and higher wages and standards of living by encouraging the IT economy.

Cloud computing is a technological paradigm that is certain to be a new engine of the global economy. But attaining those benefits will require governments around the world to establish the proper legal and regulatory framework to support cloud computing. And it will require the US to continue to lead the way. Governments must provide a solid legal and regulatory framework.

Ranking the Cloud

The move to the cloud and capitalization on its benefits across the board is hardly inevitable, and an urgent task lies ahead for governments. To obtain the benefits of the cloud, policymakers must provide a legal and regulatory framework that will promote innovation, facilitate an infrastructure to support it, and promote confidence that using the cloud will bring the anticipated benefits without sacrificing expectations of privacy, security and safety.

Earlier this year, BSA released its inaugural Global Cloud Computing Scorecard.[2] The Scorecard analyzes the laws and regulations of 24 countries in seven separate policy areas: data privacy; security; cybercrime law; intellectual property protections; support for industry-led standards and international harmonization of rules; efforts to promote free trade; and, ICT readiness and broadband deployment. It is well established that each of the individual elements of the scorecard is critical to economic growth and job creation; taken together they provide the full foundation for a robust cloud economy.

The Scorecard is a first-of-its-kind ranking of the "cloud readiness" of 24 countries that account for 80 percent of the global ICT market. But, even more importantly, the Scorecard provides a policy roadmap

[2] Business Software Alliance, *BSA Global Cloud Computing Scorecard: A Blueprint for Economic Opportunity* (2012), *available at* www.bsa.org/cloudscorecard.

for the initiatives and measures that all countries can — and should — implement to ensure that they reap the full economic and growth benefits of cloud computing.

They are especially critical in the context of cloud computing because the cloud provides a positive multiplier opportunity. Continued innovation requires the adoption of these policies. In return, cloud computing will ensure that innovation is fully harnessed and realized.

The United States finishes in fourth place globally in the Cloud Scorecard. Congress can improve on that ranking by taking steps that are widely supported in the tech community. For example, Congress should take steps to update the Electronic Communications Privacy Act (ECPA) to better reflect the changes in technology since that law was passed in 1986. BSA and a range of both industry and civil liberties groups have been calling for ECPA reform for several years. In addition, lawmakers should update laws such as the Computer Fraud and Abuse Act that are aimed against hackers and those who would attack computer networks.

It should be noted, of course, that the benefits of these updates are not limited to cloud computing. They accrue to the benefit of all technology firms – and users.

BSA's Full Blueprint for Cloud Policy Includes Seven Factors

The economic growth predicted to flow from cloud computing — and the resulting transformation of both businesses and national economies — is predicated on the proper policies being in place in each of the seven areas used in the BSA index:

- Ensuring privacy: The success of cloud computing depends on users' faith that their information will not be used or disclosed in unexpected ways. At the same time, to maximize the benefit of the cloud, providers must be free to move data through the cloud in the most efficient way.

- Promoting security: Users must be assured that cloud computing providers understand and properly manage the risks inherent in storing and running applications in the cloud. Cloud providers must be able to implement cutting-edge cybersecurity solutions without being required to use specific technologies.

- Battling cybercrime: In cyberspace, as in the real world, laws must provide meaningful deterrence and clear causes of action. Legal systems should provide an effective mechanism for law enforcement, and for cloud providers themselves, to combat unauthorized access to data stored in the cloud.

- Protecting intellectual property: To promote continued innovation and technological advancement, intellectual property laws should provide for clear protection for user interfaces and other advances reflecting innovations in cloud technology.

- Ensuring data portability and the harmonization of international rules: The smooth flow of data around the world — as between different cloud providers — requires efforts to promote

openness and interoperability. Governments should support voluntary industry-led efforts to develop standards, while also working to minimize conflicting legal obligations on cloud providers.

- Promoting free trade: By their very nature, cloud technologies operate across national boundaries. The cloud's ability to promote economic growth depends on a global market that transcends barriers to free trade, including preferences for particular products or providers.

- Establishing the necessary IT infrastructure: Cloud computing requires robust, ubiquitous and affordable broadband access. This can be achieved through policies that provide incentives for private sector investment in broadband infrastructure and laws that promote universal access to broadband.

Foreign Governments Raise Barriers to the Global Cloud

In recent weeks, BSA released a report entitled "Lockout" that examines a new wave of IT-focused market-access restrictions that are spreading through key emerging markets.[3] The report covers five types of such restrictions. One of these, in particular, threatens to undermine the global cloud economy. This particular category of restrictions involve regulatory obstacles that nations invoke in what they say are the interests of protecting data privacy or ensuring security. Far too often, though, these are purely pretextual barriers designed to benefit domestic cloud providers. For example, the report examines efforts to inhibit multinational cloud service providers with barriers including data-location requirements or restrictions on cross-border transactions.

Taken together, these barriers hinder the IT industry's ability to grow and contribute to the US and global economies. These IT-focused market obstacles can be hard to recognize. They frequently are disguised as policies to promote innovation, enhance security, or advance other domestic priorities.

One other common tactic is to question the US legal system and important US laws in order to create fear and confusion. The Patriot Act is frequently – and ominously – invoked by foreign governments and international competitors. Its powers are exaggerated and misconstrued, leaving the impression that the US government has far greater ability to access data in the cloud than any other government. This simply isn't true. But that hasn't stopped others from using the Patriot Act as a weapon against US cloud providers. Some European Union officials have expressed concern and outrage over US companies' responsibilities under the Patriot Act, and the Canadian government has asserted that organizations should avoid using services hosted outside of its territory partially because of the Patriot Act. This type of fear-mongering has had a very real – and harmful – impact on US cloud providers.

There are legitimate needs for government access to information in the cloud to protect national security, but to date it isn't clear how laws governing government requests will impact cloud service

[3] Business Software Alliance, *Lockout: How a New Wave of Trade Protectionism Is Spreading Through the World's Fastest-Growing IT Markets – and What to Do About It* (2012), *available at* http://www.bsa.org/~/media/Files/Policy/Trade/BSA_Market%20Access_Report_FINAL_WEB_062012.ashx.

providers. As data moves off-premises to cloud providers, potential adopters of the cloud are concerned about if and how information may be shared with the government, creating a barrier to adoption for the US cloud especially for foreign consumers and enterprises.

US cloud providers are working diligently to ease these fears and blunt these attacks. Efforts have been made to point out the critical privacy protections in US law and to point out that all countries have such laws to protect their citizens' safety. The US government can help in this effort as well. The State Department has taken the lead in working with foreign officials to clarify the reach and scope of US privacy protections. We applaud this work and urge the State Department to continue its advocacy. The Justice Department can aid in this effort as well by increasing transparency around the Patriot Act.

What Lies Ahead: Piracy in the Cloud?

Finally, for all the excitement and possibility that cloud computing presents, it brings challenges as well. BSA has long worked on behalf of our members to reduce traditional PC software piracy. Looking ahead to the next generation of computing, BSA is examining how piracy might occur in the cloud.

In late 2010 and early 2011, BSA interviewed industry experts and frontline technologists from our member companies and from other market sectors. We determined that cloud piracy could take at least four forms:

- End users could abuse their licenses for cloud services by sharing their account credentials. [4]
- An unscrupulous business could set up a "dark cloud" to deliver illegal software or offer software as a service without a license for redistribution.
- An enterprise could set up a private "dark cloud" for its own use — that is, to provide pirated software to its employees.
- An enterprise could use a private "gray cloud" to provide legally purchased software to more users than the license allows.

Of these four types of cloud-related IP theft, the threat of "dark clouds" and "gray clouds" in private cloud environments hosted by enterprises might prove to be the greatest long-term threat. That is because private clouds are merely efficient, scalable architectures for delivering traditional IT tools — which are typically licensed the same way whether they are installed locally for each individual user, or deployed through traditional networks or clouds.

For decades now, the most common form of enterprise software piracy has occurred when an otherwise legal company buys a license to install a program on one computer but then installs it on tens, hundreds, or thousands of additional machines. Today, in a private cloud environment, a company can centrally

[4] More recent research has found that credential sharing is common in the cloud – particularly in emerging economies where recent adopters of computers and information technology frequently move directly to cloud services. See, Piracy in the Cloud: A Picture Is Starting to Emerge, BSA TechPost, Robert Holleyman, July 19, 2012 (available at: http://blog.bsa.org/2012/07/19/piracy-in-the-cloud-a-picture-is-starting-to-emerge/).

serve the software to all of its users rather than install it on their individual hard drives. But the end result is the same: The company pays for fewer licenses than it should.

Ultimately, certain things can be counted on: Piracy will not go away in the cloud. And as cloud services continue to grow at a tremendous clip, ensuring that measures exist to protect innovators become more and more vital.

Conclusion: Ensuring a Future in the Cloud

Every day, more and more evidence points to the importance of cloud computing to the US economy and to global growth. One recent study found that public and private IT cloud services will produce nearly 14 million jobs worldwide by 2015 – and more than half of those will come from small and medium-sized businesses.[5] It goes on to predict that in that time cloud computing will generate as much as $1.1 trillion in annual revenue.

The future is clearly in the cloud, and ensuring that leadership in the cloud continues will require implementation of the right policies at home and working to ensure that other nations do the same. This is now in our hands.

[5] IDC, *White Paper: Cloud Computing's Role in Job Creation* (March 2012).

See Appendix for the attachments submitted with this statement.

Mr. GOODLATTE. Thank you, Mr. Holleyman.
Mr. Freeman, welcome.

TESTIMONY OF JUSTIN FREEMAN, CORPORATE COUNSEL, RACKSPACE US, INC.

Mr. FREEMAN. Thank you, Mr. Chairman. On behalf of both myself and Rackspace, I would like to express my appreciation for the time of this Committee and the opportunity to provide some additional insight into the key elements of cloud computing, and address some of the primary challenges of the competitiveness of American cloud providers.

Congressman Smith, I appreciate your introduction of Rackspace.

With our focus on fanatical support, which is a fierce commitment to a customer-oriented set of core values, Rackspace has grown rapidly and now serves more than 170,000 customers in 120 countries, including most global Fortune 100 companies.

Rackspace focuses on providing the cloud infrastructure and support technologies that enable the modern economy to benefit from the cost savings that cloud computing provides. Our latest focus is open stack, which is an open source cloud platform jointly developed with NASA. Open cloud technologies are the forefront of the cloud technology revolution. By fostering industry standards for cloud computing, which span multiple providers, open technologies advance security and help eliminate proprietary lock-in, which would be a requirement that cloud applications be tied to a specific provider, permitting cloud users to move their applications and data from provider to provider as they see fit.

While the phrase "the cloud" encompasses a set of technologies, services, and use cases, far too broad to go into detail here, I want to provide you with a sense of the critical elements of cloud computing. At its most basic, cloud computing is simply the use of remote computing resources, relying on the storage and processing capabilities of a remote system rather than, say, your local laptop.

We have all been using the cloud in some fashion for quite a while. Whenever we store e-mails with a web service like Gmail or Hotmail, we are essentially ceding control of that data to the cloud.

One of the most critical impacts of the cloud is of the shift to using remote shared resources, permits businesses to consume information technology in a utility or a pay-for-what-you-use model. This cost-effective delivery method makes information technology resources scalable, dynamic, and flexible, in turn driving efficiency and innovation across all sectors of the economy.

In order to continue promoting the resulting economic growth, it is essential we establish a supportive legal and regulatory environment, which is alignment with the critical cloud technologies.

We see two major barriers to the ongoing competitiveness of American cloud providers: market access issues, which were substantially informed by privacy concerns, and the exploitation of the U.S. patent system by patent trolls.

Concerns about privacy and security of data have become heightened as businesses hand off their data to systems in the cloud. And they are a major barrier to the competitiveness of American cloud companies internationally. Concerns about data privacy limits, the willingness of foreign companies to do business with United States

firms, and threatening to exclude American companies from competing abroad.

The lack of international privacy standards is a growing source of distrust amongst regulatory agencies seeking to enforce their domestic laws, and businesses struggling to ensure their compliance. There is a perception, even if unfounded, that U.S. privacy protections are insufficient to protect the data which is stored either on U.S. soil or with U.S. companies. This concern results in a reluctance by foreign companies to do business with U.S. cloud companies, and we increasingly see regulatory authorities, especially in the EU and European economic area, moving in the direction of denying U.S. cloud providers access to the European market.

It is critical to the ongoing competitiveness of American cloud companies that we take the lead and move toward to a consistent international privacy and data transfer framework while also providing clear interpretation of U.S. law which impact the obligations of cloud companies at managing the data of foreign citizens and businesses.

The second major threat to U.S. cloud providers is the exploitation of the patent system by so-called patent trolls. These are non-practicing entities which gather portfolios of patents with the sole intent of using them to extract settlements from companies unwilling to engage in expensive and protractive litigation.

These patent trolls are not protecting inventors or benefitting startups. To the contrary, a recent study calculated that their predatory tactics have resulted in the direct costs in excess of $29 billion to the industry, with approximately 40 percent of those costs formed by small and medium businesses.

Patent litigation costs routinely exceed $2 to $3 million per suit, and patent trolls seek settlement after settlement in order to artificially increase the value of a patent portfolio without any relation to its actual market value. The result is a cascading extortionist abuse of the patent system.

Cloud technologies are advancements to existing information technologies and require a fair and balanced patent system in order to remain innovative. Cloud and open technology standards cannot survive in this environment. It is essential that we protect the growing use of standardized cloud technologies, the benefits they bring, and allow cloud companies to reinvest in technologies, jobs, and innovation instead of revenue draining litigation.

We at Rackspace share your commitment toward creating successful legislation that enhances U.S. business competitiveness, while ensuring the Internet remains a free and open driver of innovation for our long-term future.

Thank you for your time. We look forward to working closely with you.

[The prepared statement of Mr. Freeman follows:]

House of Representatives

Committee on the Judiciary

Cloud Computing: An Overview of the Technology, IP and Market Access Concerns Facing American Innovators

Wednesday, July 25, 2012

Written Testimony of Justin Freeman, Corporate Counsel, Rackspace US, Inc.

Table of Contents

I. About Rackspace – Fanatical Support and the Open Cloud 3
II. An Overview of the Cloud 3
III. Major Challenges Facing US Cloud Providers 5
A. Market Access & International Privacy Policies 5
B. Freedom to Innovate & Patent Litigation 6
Appendix 1: Cloud Services 8
Appendix 2: Cloud Security 9

I. About Rackspace – Fanatical Support and the Open Cloud

Founded in 1998 and headquartered in San Antonio Texas, Rackspace is the service leader in cloud computing — a fast-growing industry that helps businesses avoid the expense and hassle of owning and managing their own computer gear by providing computing resources to them over the Internet. Rackspace now serves more than 170,000 customers in 120 countries, including most of the global corporations in the Fortune 100. More than 4,300 engineers, software programmers, customer support representatives, and others provide famed Fanatical Support, the 24/7/365 customer service and support that has defined Rackspace.

One of Rackspace's top priorities is focusing on the development and deployment of Open Cloud computing infrastructure, based on the OpenStack platform jointly developed with NASA. OpenStack is a set of open-source cloud computing technologies which are platform agnostic – meaning that a company utilizing OpenStack to run its cloud computing services is capable of migrating between a variety of hosting providers and platforms, instead of selecting only one provider and being stuck with that choice. These Open Cloud technologies represent a sea-change in cloud computing – by eliminating proprietary lock-in they help foster critical industry standards for cloud computing and create a robust ecosystem of services which span multiple cloud providers. Much like a cell phone that a user can take from carrier to carrier, applications built on an OpenStack infrastructure can easily be moved between hosting providers.

II. An Overview of the Cloud

At its heart, cloud computing is nothing radically new. "Cloud" essentially describes the use of remote computing resources, whether it be storing information remotely (such as by utilizing a web based email account to store emails in a providers cloud, rather than on a local laptop), or processing information remotely (which occurs when a user leverages the processing power of a remote computer to perform calculations – power which may not be available at a local laptop). These two fundamental computing resources, *storage* and *compute*, are the essence of modern information technology.

What is new is the ubiquitous availability of remote connectivity which drives the cloud revolution. During the first stages of the IT revolution, corporations deployed massive mainframes which handled all the storage and compute needs of users, who accessed these remote resources through terminals. Although few consider this cloud computing, because all the systems were local and required a physical link, the terminal-mainframe model informs modern cloud computing approaches.

As modern workstations increased their storage and processing capabilities, an increasing amount of work was done exclusively on a user's local computer. Even in the early days of the internet, most storage was local, and local compute power was all that a user had access to. Contrast with today's cloud, where applications are consumed as remote resources, rather than software running on a local device.

Along with the cloud we now see the commoditization of storage and compute resources, permitting companies to save substantial amounts of capital by paying for modern IT

costs on a utility basis, just like electricity consumption, rather than invest in large capital expense "homegrown" IT infrastructure. This utility model is the blessing of the modern cloud – it permits IT resources to be dynamically allocated as needed, and allows services to be delivered over the internet to almost any user on any device (whether a laptop, cell phone, or tablet). The enhanced user experience and savings drive modern innovation in virtually all sectors of the economy.

The flexibility of IT models has resulted in a lot of confusion regarding what constitutes a cloud. There is no concrete definition – "cloud computing" has become an expansive term encompassing types of infrastructure (dedicating servers to one company's use, or sharing them to maximize cost savings) and types of services (such as remote email, or remote office applications like Microsoft's Office 365).

Clouds come in various types and shapes, the configuration of the underlying servers and devices constitutes the infrastructure of the cloud. While the potential recombination is substantial, there are fundamentally three different types of cloud infrastructure:

- **Dedicated Clouds** comprised of physical infrastructure dedicated to one company's use. That company controls the servers and storage devices exclusively. Also known as private clouds, these are the "single family homes" of the cloud. Dedicated clouds can be located anywhere – at a company's corporate headquarters or at hosting providers data center.

- **Public Clouds** made up of shared servers whose resources have been virtually partitioned by user. These are the "apartments" of the cloud – all users rely on the same set of underlying devices, and a provider typically manages the segregation of those resources by user. These are the most cost effective types of cloud infrastructure, as the overall capital costs are shared amongst the users, who typically pay only for what they use. Because of their shared nature, public clouds are almost always maintained by a hosting provider at premises that it operates.

- **Hybrid Clouds** come in two flavors, and represent the majority of modern IT usages. A company may split its user of cloud resources between resources dedicated to its use (a dedicated cloud) and resources it shares (a public cloud) in order to balance the need for control provided by dedicated clouds with the cost savings of public clouds. A company may also make use of some computing resources which it runs at its own offices, and some which it outsources to a hosting provider. This balancing act often results as a trade-off between security, control, and cost.

These "different types of clouds" reflect different configurations of computing resources, which are then used to provider different types of services in a 'pay as you go' approach. Cloud service models often scale control with cost, and reflect different methods of delivering services through the cloud in a utility pricing model. For a more detailed review of the types of cloud services and their impact on control, please see Appendix 1.

Although the types of resources used by the cloud are not novel, the combination of choice and the ability to hand-off control of IT resources at various levels is. Ultimately,

securing the cloud requires you to know who is in charge of what layer of security, and what they are doing about it (how are they protecting your data?). The fundamentals of IT security are quite similar in the cloud, the focus of a responsible cloud user should be on ensuring that at each layer of cloud security, appropriate controls are in place. Ultimately, the party which controls the data has the most fundamental level of security responsibility – they can encrypt sensitive data and thereby truly protect it from malicious or unauthorized access. For an introduction into the fundamentals of cloud security, a discussion of appropriate cloud security controls, and examples of data types and applicable regulations, please see Appendix 2.

III. Major Challenges Facing U.S. Cloud Providers

The United States is home to the most innovative IT sector in the world, and is especially vibrant when it comes to adopting and innovating in the Cloud. Unfortunately, market barriers resulting from globally inconsistent data protection standards threaten the ability of U.S. companies to compete internationally. Moreover, patent trolls (also known as non-practicing entities or NPEs) are attempting to monetize questionable patents in an all out legal assault directed at the cloud computing industry. It is impossible to overstate how critical market access and an innovative environment are to the ongoing success of the U.S. cloud services industry.

A. Market Access & International Privacy Policies

Many U.S. cloud technology companies are attempting to compete overseas. Much of the time these services are provided out of a U.S. based datacenter to remote users – a position which is increasingly met with opposition from foreign countries concerned about friction between their domestic privacy principles and U.S. law. U.S. cloud providers and technology companies are facing a growing threat to their ability to compete internationally in the form of uncertainty and misrepresentation about their ability to protect and secure data.

EU countries are required to adhere to the principles (implemented differently in each member state) of the EU Data Privacy Directive, a set of requirements intended to protect the rights and privacy of citizens of the EU member countries. EU law currently mandates specific requirements regarding the treatment of data regarding citizens of the member states, including required notifications if the data is shared with third parties. Unease about the U.S. Patriot Act, which requires U.S. companies to comply with U.S. government data requests is driving EU business and regulatory concerns about doing business with U.S. companies.

Cloud sales in Europe trail those in the U.S. by almost 2 years, in part because of these concerns.[1] At Rackspace we routinely face concerns by potential customers based in the EU

[1] Kevin J. O'Brien. "New European Guidelines to Address Cloud Computing." The New York Times, July 1, 2012, Technology Section. Available at: https://www.nytimes.com/2012/07/02/technology/new-eu-guidelines-to-address-cloud-computing.html?_r=1&pagewanted=all.

that their mere utilization of cloud services by Rackspace (even in a European data center) would place them in violation of applicable EU regulations. The same uncertainty is appearing in the Indian market, as recent privacy reforms there aligned closely with the EU Data Privacy Directive. The lack of a consistent international privacy regime has resulted in uncertainty that is crippling the ability of U.S. cloud companies to access and compete in international markets.[2]

EU regulatory authorities are increasingly moving in the direction of denying U.S. cloud providers access to EU markets as a result of this uncertainty. Privacy concerns all too often poison competitiveness as they become the foundation of protectionist measures. U.S. healthcare IT companies have already seen this occur in the form of Canada's FOIPPA healthcare privacy law, which prohibits Canadian healthcare providers from storing patient data on systems located in the U.S. Distrust of U.S. privacy standards by EU regulatory authorities is often general in nature, without a specific legal reasoning or regulatory provision to blame. It is critical that the U.S. government take steps to allay business unease with the unclear regulatory environment and to quash protectionist impulses in the cloud computing market.

It is essential to move towards a consistent international privacy and data transfer framework, while simultaneously providing clear interpretations of U.S. laws which may impact the obligations of U.S. companies serving international customers.

B. Freedom to Innovate & Patent Litigation

Even relatively established cloud computing companies rely on rapid innovation for their success, and the freedom to innovate is critical for nascent cloud technology and service providers. The U.S. patent system is increasingly abused by patent trolls which gather complex software and business practice patents with the sole intent of extracting payments from truly entrepreneurial companies.

The direct costs of this abuse of the patent system are staggering: reaching approximately $29 billion in in 2011 alone.[3] That number is exclusive of the related and often crippling business impact these actions impose on innovative companies such as resource diversion, product delays, and losses of market share.[4] These costs are a pure social loss – not the result of a repayment to an inventor or a small company whose innovations were unjustly exploited. Instead these lawsuits routinely target large and small operating companies similarly; the only net beneficiaries are the aggressive non-practicing entities which originate these lawsuits. In fact, a substantial number of small and medium businesses are targeted - they comprise about 90% of the companies sued, and their portion of these costs is near 40% of the total.[5]

---

[2] Patrick Baillie. "Can European Firms Legally Use U.S. Clouds To Store Data?" Forbes, January 2, 2012. Accessed July 23, 2012. Available at: http://www.forbes.com/sites/ciocentral/2012/01/02/can-european-firms-legally-use-u-s-clouds-to-store-data/.

[3] James E. Bessen & Michael J. Meurer. "The Direct Costs from NPE Disputes." Boston Univ. School of Law, Law and Economics Research Paper No. 12-34. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2091210.

[4] *Id.*

[5] *Id.*

The cloud industry is under siege. Computing services companies are routinely one of the industries most impacted by patent troll litigation, and the high-tech sector consistently accounts for more than half of all such suits filed.[6]

While recent efforts to reform the patent system have addressed many long-standing problems, the patent trolls have continued their predatory litigation, and further reform is necessary. Focusing on the behavior of the entity, rather than its status a simply a non-practicing entity is a promising way forward.[7] Fee shifting to favor defendants in cases brought by non-practicing entities, strict limitations on the applicability of notoriously difficult to interpret software and business method patents, and alignment of awards with the value of the underlying patent are potential approaches to this problem.[8] Absent reform, it is clear that aggressive patent litigation will continue to constrict the resources of well established companies, while exerting a potentially decimating impact on the innovative small and medium businesses the patent system is intended to protect.

[6] Patent Freedom. "Exposure by Industry." Data captured as of July 13, 2012. Available at: https://www.patentfreedom.com/about-npes/industry/

[7] James E. Bessen & Michael J. Meurer. "The Direct Costs from NPE Disputes." Boston Univ. School of Law, Law and Economics Research Paper No. 12-34.

[8] *Id.*

Appendix 1: Cloud Services

Types of Services

The different types of clouds (configurations of computing resources) are used to deliver different types of service models. These service models scale control with cost, and are different methods of delivering services in a cost effective utility model. As a user moves from consuming IT resources in the form of dedicated devices (such as servers in a company data center) to consuming IT resources as a service they gradually cede control to providers and third parties.

- **Infrastructure as a Service (IaaS)**: In this most fundamental type of IT service, providers control the datacenter, the network, and physical access to servers and storage devices. Users control the rest, and are often responsible for their administration of the IT resources. Most IaaS providers will not permit their customers physical access to devices – all their users share the same physical location, although many of the actual devices are dedicated to particular users rather than shared.

- **Platform as a Service (PaaS)**: In the platform model, the provider controls the infrastructure (which of course may be subcontracted) and deliver systems ready to run user's applications. Users bring their applications and data and run them on a ready-to-go platform managed by the provider.

- **Software as a Service (SaaS)**: In a SaaS model the underlying IT resources are obfuscated from the user, and the provider delivers a ready-to-use application, maintaining responsibility for the underlying platform and infrastructure. This is the most common type of cloud service for consumers (gmail & Office 365 are great examples – the user consumes and email or office application, without having the software installed locally), and is increasingly relied on by businesses looking for customized off-the-shelf applications, without having to make substantial investments in new computing infrastructure.

Appendix 2: Cloud Security

Fundamentals of Cloud Security

Ultimately, securing the cloud requires you to know who is responsible for each aspect of the cloud resources, and how each layer of security is being addressed. There are three fundamental levels of security in the cloud:

- **Physical Security**: This most fundamental layer relates to having physical access to the IT appliances. If the servers running a cloud are not physically secured from unauthorized access then there is little else that can be done. A malicious party with physical access to a server can readily engage in obvious sabotage such as data theft (even as simple as removing the physical hardware) and physical damage causing data loss, as well as more complicated security risks, such as injecting malicious code or viruses through a thumb drive.

- **Network Security**: It is critical to secure networked systems both from local threats (other users on the same network, including other employees in the same office for example) and remote threats (malicious attacks over the internet). Network security in the cloud is often split amongst multiple parties, so it is especially important for a security conscious user to understand who is responsible for what portion of the network. Insecure networks can permit unauthorized access, the injection of malicious code and viruses, to the more common denial of service attack – where a third party shuts down the ability of servers to function by overwhelming their network capabilities, without necessarily engaging in theft.

- **Logical Security**: The broadest layer of security, logical security relates to controlling user permissions and securing applications from vulnerabilities. Controlling who can get to what based on their access credentials is a fundamental requirement for a secure system. Role based access restrictions are a mechanism of getting users access to the data they need (like quarterly financial statements) while keeping them out of data they don't (like HR records). It also relates to the security of the applications users run – the most common security gap occurs when a user fails to update their operating systems (such as with Microsoft's routine patches) or their anti-virus definitions (without constant updates, anti-virus programs can easily become obsolete).

Selecting the Right Cloud Provider

In order to build a secure cloud, it is essential to select the right cloud infrastructure, select the right provider, review the providers security and operational controls, and to ensure sensitive data is always encrypted.

- **Selecting the right cloud infrastructure**: while an infrastructure dedicated to a single user is typically the most secure, public clouds formed of shared resources can be just as

secure. The key element is identifying how data is secured, regardless of the type of cloud it resides in.

- **Selecting the right provider**: It is critical that cloud users have a clear understanding of the security practices undertaken by their providers, and that the providers are willing to demonstrate compliance with their controls. There is an incredible number of potential combinations of security responsibilities, so users must make sure they choose a combination that meets their needs and capabilities.

- **Reviewing security controls**: It is increasingly common to require a third-party audit of a provider's security controls, achieving both confidence in the provider and often in order to meet regulatory requirements. Three common audit and control reports are the SSAE16 (a third party review of a company's ability to meet its stated operational controls), a PCI-DSS audit (commonly utilized in the payment card transaction industry), and a Safe Harbor Self-Certification (especially critical in business ventures between U.S. and EU businesses).

- **Encryption, encryption, encryption**: Regardless of who is responsible for the layers of security, there is only one fundamental method of securing data: encryption. Encryption ensures that even when a system is breached (which increasingly seems like an inevitability even with the best security practices in place) the attacker is unable to utilize any data stolen, mitigating the risks to privacy (in the case of personal information), competiveness (in the case of proprietary business information), and national security or defense (in the case of military information).

Examples of Regulated Data Types

Cloud users should be especially sensitive to regulatory requirements (whether industry or governmentally based) regarding the types of data they store in the cloud. Below are some examples of the different types of data commonly stored in the cloud and applicable U.S. regulations.

Data Types	Examples	Example Regulations
Personally Identifiable Information (PII)	Credit Card Processing Information	PCI-DSS, Gramm-Leach-Bliley
Protected Health Information (PHI)	Health Records	HIPAA/HITECH
Sensitive Corporate Governance Data	Corporate Audit & Financial Reports	Sarbanes-Oxley
Sensitive Business Information	Forecasts, Development Plans, Strategic Proposals	None – High Economic Value
Generally Public / Non-Sensitive Information	Marketing Collateral, Miscellaneous Documentation	None – Low Economic Value

10

Mr. GOODLATTE. Thank you, Mr. Freeman.
Mr. Chenok, welcome.

TESTIMONY OF DANIEL CHENOK, EXECUTIVE DIRECTOR, CENTER FOR THE BUSINESS OF GOVERNMENT, INTERNATIONAL BUSINESS MACHINES CORPORATION (IBM)

Mr. CHENOK. Thank you, Chairman Goodlatte, Ranking Member Watt, Chairman Smith, and the entire Subcommittee.

Mr. GOODLATTE. You may want to turn your microphone on there and pull it close.

Mr. CHENOK. Will do. Thank you, Chairman Goodlatte, Ranking Member Watt, Chairman Smith, and the Subcommittee for the opportunity to speak today. And thank you for the introduction earlier.

I am Dan Chenok, Executive Director of the IBM Center for the Business of Government. The center helps government executives improve the effectiveness of their agencies and programs and has addressed cloud computing from a number of perspectives over the past few years. My testimony today draws on this and other experience with the growth of cloud computing.

Moving the cloud brings numerous demonstrable and positive outcomes, such as cost savings, shared resources, increased program effectiveness, energy and environmental improvements, and, as others have noted today, innovation.

I will focus today on three key issues that we see cloud can best be leveraged now and in the future. First, how to implement cloud efficiently, second, how best to address security, and third, how to leverage the cloud's global model effectively.

The key for success with cloud implementation is a strategy to define how to increase efficiency, save costs, and improve performance of programs in the cloud. A small investment in up front planning can pay large dividends in measured outcomes from any cloud migration because most entities integrate cloud into their existing legacy environments. They must make choices as to what technologies, processes, and data should migrate to the cloud over what period of time and at what cost.

I would note that the Federal Government has already begun to realize the benefits of cloud computing. Movement to the cloud can fundamentally transfer how Federal agencies leverage IT. And efforts such as the OMB cloud strategy and GSA FedRAMP initiatives are spurring progress. Our center has produced papers on cloud implementation available at our website, www.businessof government.org.

With respect to security, despite perceived concerns about security risks, cloud can provide for an environment that is superior for applying many critical security measures. Centralizing data storage and governance in the cloud can actually provide better security at a lower cost than is the case with traditional computing environments.

Moreover, cloud can improve certain key security practices, such as detection of threats, remediation to minimize those threats, prediction of where threats may occur next, and protection of data and devices.

Regarding the global model, the benefits of cloud computing increase when providers can move computing and data power to locations that are most cost-effective rapidly and with no loss of service quality or security. Real time movement of computing resources

points out the need to understand, as others have noted today, issues involved in cross-border data flows in the cloud. Most issues in this space are best addressed via contracts between parties who can designate jurisdiction and establish clear provisions for ownership, privacy, and security.

I would like to highlight several issues that impact the cloud's global nature. These areas are the extent to which government can access data across borders, international privacy collaboration, and open standards.

The extent to which government can access data across borders can be a subject of confusion among cloud providers and users. However, as has been indicated today, many nations have similar domestic data policies. A recent white paper from the law firm Hogan Lovells found that each of the 10 countries studied vests authority in the government to require a cloud service provider to disclose customer data in certain situations. And in most instances, this authority enables the government to access data physically stored outside the country's borders.

And as Chairman Smith indicated in his opening remarks, this study also indicated that in a number of cases, protections from government intrusion in the U.S. were actually greater than in other countries.

Regardless of jurisdiction, individuals whose data resides in the cloud will have greatest confidence if, to the extent permissible under law, they do not lose protection solely based on where their data is stored and processed.

Cloud computing would also benefit from an international regime that promotes privacy and supports efficiency cross-border data flows. While complete harmonization of rules is not practical or desirable, countries may be able to recognize each other's rules, including privacy safeguards.

Finally, the benefits of cloud can best be achieved by reliance on open standards that promote data portability and interoperability, which are critical for successful adoption and delivery of cloud-based solutions. An open standards approach would also help to address location-based mandates. While certain practices by governments to locally-sourced cloud computing may be understandable, governments could enhance the cloud's efficiency and cost-effectiveness by avoiding local mandates and leveraging and encouraging an open global model.

Chairman Goodlatte, Ranking Member Watt, Chairman Smith, the Subcommittee, thank you for the opportunity, and I welcome any questions.

[The prepared statement of Mr. Chenok follows:]

Prepared Statement of Daniel Chenok, Executive Director, Center for The Business of Government, IBM

Good afternoon, and thank you Chairman Goodlatte, Ranking Member Watt, and the entire Subcommittee for the opportunity to speak with you about cloud computing.

I am Dan Chenok, Executive Director of the Center for The Business of Government at IBM. The Center connects public management research with practice. Since 1998, we have helped public sector executives improve the effectiveness of government with practical ideas and original thinking. We sponsor independent research from the academic and non-profit sectors, and we create opportunities for dialogue

on a broad range of public management topics. The Center has addressed cloud computing from a number of perspectives over the past few years.

I also serve as Chair of the Information Security and Privacy Advisory Board, which is the chartered under the Federal Information Security Management Act (FISMA) to advise the government about information security and privacy issues affecting civilian Federal agencies, and has addressed security and privacy issues involved in cloud computing.

My testimony today draws on this and other experience that I have had with the growth of cloud computing, primarily with respect to how government can best promote the efficient, secure, and cost-effective use of this technology. After addressing context and benefits, I will focus on three key issues that impact how cloud can best be leveraged, now and in the future.

CONTEXT

Many descriptions of cloud computing are cited across government and industry, including a formal definition from the National Institute of Standards and Technology (NIST). I would offer that the cloud includes environments where physically distributed computing resources—including infrastructure, applications, or databases—connect in real time to help a company, consumer, or government agency perform a transaction, service, or inquiry.

Cloud services can be provided over the public Internet, but can also be done through connections over networks that run independently. Government agencies often establish clouds independent of the open Internet due to perceived risks of making data available over public channels—but the government is moving in the direction of more use of the open Internet for cloud as well.

Indeed, whether consumers, companies, and governments realize it, they are already in the cloud all the time. Many popular email services, including Gmail, Hotmail and Yahoo, function over the distributed networks that constitute the cloud, and provide access to millions of people. Businesses and governments are increasingly using the cloud for email as well.

BENEFITS OF THE CLOUD

Cloud computing is much in the news and lexicon these days. Questions about the cloud include: does cloud help end users, will cloud help businesses and federal agencies carry out their mission, and will cloud reduce costs? The answer to all of these questions is "yes."

Moving to the cloud brings numerous demonstrable benefits:

- **Cost Saving**. Cloud computing allows customers to pay for just the computer resources that they use. They can avoid both a large initial upfront expenditure in hardware and software, and ongoing operating and maintenance expenses for their own IT. Resource usage can be monitored, controlled, and reported in a transparent way for both the provider and consumer of the cloud service. Indeed, a Brookings Institution study found that ". . . agencies generally saw between 25 and 50 percent savings in moving to the cloud;" this same report refers to other studies which claim savings from 39% to 99%. (http://www.brookings.edu/~/media/research/files/papers/2010/4/07%20cloud%20computing%20west/0407__cloud__computing__west)
- **Increased Effectiveness.** Network outages are an ongoing challenge for IT departments. Cloud computing can offer a higher level of service and reliability, reduce the harm that can come from network outages, and provide for a more immediate response to emergency situations by enabling real-time transfer of IT services to areas that are not affected by emergency.
- **Optimized Computing Usage.** IT service providers see cloud computing not only as a means to better serve their customers, but also to optimize data center usage. In many centers, only a small fraction of computing capacity is used at any time; the remaining capacity sits idle. Cloud enables flexible scaling across customers based on demand, which increases capacity and cost-effectiveness.
- **Energy and Environmental Improvements.** While most computers and servers are certified as energy efficient, cloud takes green computing one step further—decreasing electricity use, slashing carbon emissions, and reducing IT costs through cost-effective use of computer and network infrastructure. Cloud also opens avenues for telecommuting (e.g., through internet-based email), which brings added environmental benefits.
- **Innovation and Transformation**. Cloud computing can help to spur innovation and transform operations. In the next several years, andthe use of the

cloud to pave the way for for business model innovation is likely to increase significantly—innovation that includes entering new lines of business, reshaping an existing industry, or transitioning into a new business role.

In addition, and as has been noted by both the current and previous Federal Chief Information Officers at the Office of Management and Budget (OMB), Federal computer users have lagged behind industry in IT productivity gains from IT, with outdated applications and burdensome rules governing acquisition and management of IT services. Movement to the cloud can fundamentally transform how federal agencies leverage IT, and to make federal workers far more effective in their use of IT.

The Federal government has, of course, already begun to realize the benefits of cloud computing. Examples include:

- the development and implementation of governmentwide and specific cloud strategies from OMB and agencies,
- the recent introduction of the General Services Agency (GSA) Federal Risk and Authorization Management Program (FedRAMP) program that fosters interoperability in cloud services across agencies. Indeed, other governments are studying FedRAMP's implementation closely to possibly emulate the model; and
- work by the National Institute of Standards and Technology (NIST) to clarify and guidance on the cloud.

KEY ISSUES FOR DISCUSSION

Today, I would like discuss three main challenges for government in order to realize the full benefits of the cloud:

- how to implement cloud efficiently,
- how best to address security in the cloud, and
- how to leverage the cloud's global model effectively.

Implementation

Key for success in any cloud implementation is a strategy to define how to increase efficiency, save costs, and improve performance of programs in the cloud. A small investment in upfront planning can pay large dividends in measured outcomes from any cloud migration. This is especially important because most entities do not build brand new computing environments where all activities operate in the cloud. Rather, they integrate cloud-based infrastructure, applications, and services into existing legacy environments, and must make choices as to what technologies, processes, and data should migrate to the cloud, over what period of time, and at what cost. To guide those choices, organizations need a sound up-front strategy that considers investments relative to resource availability and mission objectives.

The IBM Center for the Business of Government has produced a number of papers that address cloud implementation, especially in the Public Sector. For example:

- In a 2009 report for the Center, "Moving to the Cloud: An Introduction to Cloud Computing in Government," David Wyld provides non-technical executives with a roadmap to understand key questions to ask as their organizations move to the cloud. He frames key challenges facing government leaders in the space, including scalability, security, open standards, procurement, and legal issues.
- In 2010, author Costas Panagopoulos wrote in our semi-annual journal, *The Business of Government,* about the lessons learned in cloud implementation by the Census Bureau ("Counting on the Cloud: Early Reflections on the Adoption of Cloud Computing by the U.S. Census Bureau"). He outlines key lessons that include the need to start early in cloud design, to partner with other adopters, and to correct problems as soon as they arise.
- Many perspectives on how best to implement cloud appear on our blog site, concentrated primarily in "Strategies to Cut Costs and Improve Performance." (http://www.businessofgovernment.org/blogs/cut-costs-and-improve-performance)

In addition, much research and experience demonstrates that to maximize the cloud's benefits, organizations must move aggressively to adopt more standardized offerings across organizations. That is, they must change current technology, procurement, and business processes to conform to best commercial practice, rather than modifying the cloud to fit existing organizational processes. Standardized offerings provide economies of scale and allow providers to automate processes that result in lower costs for users.

In addition, while savings can be achieved by migrating current applications, not all existing applications can run in a cloud efficiently. Organizations can collect data on how applications are being used to make informed decisions about which applications to migrate to the cloud, and in what order. This data can also help to sunset unneeded applications and optimize IT more efficiently and effectively.

Finally, cloud implementation can enable innovation. Developers who come together over cloud-based platforms that rely on open standards can share ideas and test approaches in ways that take advantage of the wisdom of many, rather than the few who work on a custom application.

Security

Relinquishing direct control of the IT infrastructure by adopting the cloud has raised perceived concerns about security risks. Cloud computing, however, can provide for an environment that is inherently superior for applying many critical security measures. By centralizing data storage and governance, clouds can actually provide better security at a lower cost than can traditional computing environments. Cloud environments can also provide differentiated levels of security, reflecting the fact that some data requires a great deal of protection while other data requires far less. Cloud providers can work with their customers to deliver security efficiently and effectively based on different levels of risk—security services can be built into the cloud up front to optimize protection at a given risk level.

Moreover, by facilitating uniform management practices across a distributed computing environment, cloud can improve certain key security practices, such as:

- **Detection**—the cloud creates the ability to link together millions of security nodes on the net. By working together, these nodes can better detect new threats how to implement cloud efficiently.
- **Remediation**—Quick remediation is vital for cyber security—the less time the malware is present, the better the protection. The cloud allows implementation much more rapidly than the older model of having to load the solution onto multiple machines.
- **Prediction**—Increasingly, cyber security focuses on limiting the ability of bad actors to act in the first place. The cloud helps security teams to identify machines that create and disseminate malware, and to quickly isolate those machines—blocking their ability to infect customer systems.
- **Data and Device Protection**—A significant security threat, and one that has impacted the Federal government, is breach of data, especially from lost or stolen laptops or mobile devices. Cloud provides for centrally stored data with continuous and automated network analysis and protection, so that if a device is lost, the data and applications are not lost with it (unless the user has been allowed to load them separately onto the device).

As noted earlier, I also Chair the Federal Information Security and Privacy Advisory Board (ISPAB). Building off a Board-hosted forum on best practices in this space several years ago, the ISPAB has highlighted numerous ways that the Federal government can best addresses security in the cloud, especially with regard to the operation of the FedRAMP program and the monitoring of traffic that flows in and out of agencies over cloud-based applications (see more at http://csrc.nist.gov/groups/SMA/ispab).

Global Model

The cloud can be either localized or global in nature. The benefits of cloud computing increase, however, when providers can move computing and data power to locations that are most cost-effective, rapidly and with no loss of service quality or security. For example, consider the recent storm and power outages in Washington, DC—in a situation like this, using a cloud that allows the online relocation of computing resources would provide continuity of service far more quickly and cheaply than a platform restricted to local computing locations.

Real-time movement of computing resources points out the need to understand issues involved in cross-border data flows in the cloud. Of course, data has moved across borders for decades—airlines, pharmaceuticals, telecommunications, and technology companies are among those with long history here. The cloud has amplified attention to cross-border data flow issues such data sovereignty and jurisdictional questions. Most of these issues are best addressed via contracts between solution providers and customers; contracts can designate jurisdiction and establish clear provisions for ownership, privacy, security, and consumer protection.

I would like to highlight some recent findings and observations in three areas that affect the cloud's global nature and American competitiveness in this space—the extent that government can access data across borders, international privacy collaboration, and open standards.

Government Access to Data

The extent to which governments can access data across borders is a subject of confusion among cloud providers and users. However, many nations have similar domestic data policies. A recent HoganLovells White Paper, "A Global Reality: Governmental Access to Data in the Cloud," reveals that U.S. law provides some greater privacy protections:

> "In jurisdictions outside the United States, there is the real potential of data relating to a person, but not technically "personal data," stored in the Cloud being disclosed to governmental authorities voluntarily, without legal process and protections. In other words, governmental authorities can use their "influence" with Cloud service providers—who, it can be assumed, will be incentivized to cooperate since it is a governmental authority asking—to hand over information outside of any legal framework. United States law specifically protects such data from access by the government outside of legal process."

Furthermore, the paper notes that "it is not possible to isolate data in the Cloud from governmental access based on the physical location of the Cloud service provider or its facilities. Governmental access to data in the Cloud is ubiquitous, and extends across borders." As the paper concludes, a detailed analysis of ten countries revealed that:

> "every single country that we examined vests authority in the government to require a Cloud service provider to disclose customer data in certain situations, and in most instances this authority enables the government to access data physically stored outside the country's borders, provided there is some jurisdictional hook, such as the presence of a business within the country's borders. Even without that "hook," MLATs allow access to data across borders." [Governments cooperate with each other through "mutual legal assistance treaties" (MLATs)]

Regardless of jurisdiction, individuals whose data resides in the cloud will have greatest confidence if, to the extent permissible under law, they do not lose protection solely based on where their data is stored and processed.

International Privacy Collaboration

With the understanding that many nations have similar laws and that where a company stores its data should not reduce protections, consumers, enterprises, and governments can look at cloud providers' experience with providing security and privacy protections in order to make informed decisions about how to use applications in the cloud.

In addition, cloud computing would benefit from an international regime that promotes privacy while supporting the efficient flow of data across borders. While it is neither practical nor desirable to seek the complete harmonization of rules, countries may be able to recognize each other's rules (including privacy safeguards) to the greatest extent possible, and to honor those rules through means such as contracts and service level agreements (SLAs). This approach to interoperability would not require the same laws in each jurisdiction, but it would allow data and computing transfers to take place over the cloud based on shared understanding of how law and policy should apply.

Initiatives such as the US–EU safe harbor, the use of binding corporate rules, and the cross-border privacy initiative in APEC serve as building blocks for such an interoperable international privacy regime. The benefits of such a regime would extend beyond cloud computing; they would support any entity that builds data centers in different jurisdictions. But because cloud computing relies heavily on the efficiencies gained from real-time data flows across different countries, the adoption of an interoperable privacy regime would facilitate cost-effective adoption.

Open Standards

The benefits of cloud can best be achieved by reliance on open standards that promote data portability and interoperability, which are critical for successful adoption and delivery of cloud-based solutions. Open standards enable users to reap value from a diversity of cloud providers, and to move data and applications based on a

choice of available applications without friction. Consider the analogy to Internet-based computing since the 1990s: the Internet has seen phenomenal growth and spurred so much innovation because its networks dependent largely on open standards—no one company or handful of companies has a dominant position and can single-handedly determine its architecture and development.

An open standards approach would particularly help to address the issue of location-based mandates. Over a dozen countries have recently drafted or are considering laws that would mandate in-country location of cloud data servers and storage facilities. The Business Roundtable recently released a report, "The Growing Threat of Local Data Server Requirements" (http://businessroundtable.org/uploads/studies-reports/downloads/Global_IT_Policy_Paper_final.pdf), which provides details on this issue. While certain practices by governments to locally source cloud computing are understandable—for example, for a country's national security information—governments could enhance the cloud's efficiency and cost benefits by avoiding location mandates, and leveraging and encouraging an open, global model.

CONCLUSION

Cloud computing has great promise to enable consumers, businesses, and governments to reduce IT costs and improve IT performance. Key considerations in leveraging the benefits of the cloud include implementation, security, and leveraging the efficiencies of the global model. Greater education, investment and appropriate incentives can allow government and businesses to help all stakeholders use the cloud most effectively.

Chairman Goodlatte and Ranking Member Watt, thank you for the opportunity to speak with the Subcommittee. I welcome the chance to answer any questions that you may have.

Mr. GOODLATTE. Thank you, Mr. Chenok.

Mr. Castro, we are pleased to have your testimony.

TESTIMONY OF DANIEL CASTRO, SENIOR ANALYST, INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION (ITIF)

Mr. CASTRO. Thank you. Chairman Goodlatte, Ranking Member Watt, Chairman Smith, and Members of the Subcommittee, I appreciate the opportunity——

Mr. GOODLATTE. Could you put that microphone——

Mr. CASTRO. There we go. Chairman Goodlatte, Ranking Member Watt, Chairman Smith, and Members of the Subcommittee, I appreciate the opportunity to discuss cloud computing with you today.

I would like to focus my remarks on two principles that policymakers should keep in mind with regards to cloud computing. The first principle is cloud neutrality. Cloud computing is an important trend for how organizations use information technology, but the technology itself is not so different from other forms of computing that there is a need to create cloud specific regulations. That does not mean there are not important policy issues that affect cloud computing. For example, one important issue is addressing the complex jurisdictional questions that arise from having data subjects, data owners, and service providers under different legal jurisdictions and facing conflicting regulations.

Meaningfully addressing these issues may eventually require countries to develop agreements on questions of jurisdiction or standardize some data practices, or, alternatively, advances in technology that allow data policies to actually bundle with data, and ensure that these policies are enforced may help resolve some of these questions.

While all these issues are important for many cloud computing companies, they are not necessarily unique to the technology. How-

ever, creating cloud neutral policies will require some change to ensure that laws and regulations do not favor or disfavor cloud computing.

One important step Congress can take in this direction is to update the laws that govern the electronic surveillance of data. The Electronic Communications Privacy Act was enacted in 1986, and has not kept pace with the advancement of technology and the growth of cloud computing. As a result, there are different levels of protection afforded to the privacy of an individual's data depending on where and for how long the data has been stored. Consensus is forming around the idea that reform is needed in this area to protect Fourth Amendment rights.

The second important principle for cloud computing is for policymakers to address anti-competitive foreign practices that challenge the dominance of cloud computing service providers in the United States. As a leading provider of cloud computing, U.S. companies stand to benefit tremendously from the large expected growth in cloud computing worldwide. Not surprisingly, other countries are aggressively challenging U.S. leadership in this market.

While fair competition is legitimate, some countries are using unfair policies to intentionally disadvantage foreign competitors and grow their domestic cloud computing industry. The rise of cloud mercantilism is an emerging threat to the global trade and information technology.

Some countries are using data security and data privacy regulations to create geographic restrictions on where cloud computing service providers can store and process data. Other countries have policies that explicitly require cloud computing service providers to operate data centers domestically. These requirements have the effect of making cloud computing less efficient since decisions about where to locate data centers or how to operate them must be made on political mandates rather than technical or economic factors.

Localization requirements also serve as a form of protectionism for domestic cloud computing providers since it may not be economically viable for a foreign competitor to build a domestic data center. Examples of this type of behavior can be found in many countries, for example, Greece, Vietnam, and Brunei have all passed laws which require data generated within the country to be stored on servers within those countries. Both the Norwegian and the Danish protection authorities have issued rulings to prevent the use of certain cloud computing services when those servers were not located domestically. The government in Kazakhstan issued an order to require that all dot.kz domain names operate on servers located within the country. China, Russia, Venezuela, and Nigeria have all passed localization requirements ostensibly to protect national security and payment processing. And similar types of laws are pending in other countries, including Indonesia, Malaysia, and Ukraine.

Strong U.S. leadership is necessary to combat the unfair trade practices that other nations are using to block foreign competitors in the rapidly-growing cloud computing industry. First, the U.S. government should clearly and definitively state its opposition to local data center requirements and highlight instances of non-compliance by foreign governments. For example, this type of behavior

could be highlighted by the USTR in a Special 301 report. Second, the U.S. government should affirm its intention to refrain from imposing its own local data center requirements. These policies may be tempting, but they diminish the capacity of the United States to hold other countries accountable for similar forms of protectionism.

The long-term goals of the U.S. government should be to work toward eliminating geographic restrictions on cross-border flows of data. U.S.-based cloud computing service providers have the most to lose if these type of areas become widespread. After all, the domestic market for cloud services is much smaller than the global market.

Thank you, and I look forward to your questions.

[The prepared statement of Mr. Castro follows:]

Daniel Castro

Senior Analyst

Information Technology and Innovation Foundation (ITIF)

"Cloud Computing: An Overview of the Technology and the Issues Facing American Innovators"

Before the

Committee on the Judiciary

Subcommittee on Intellectual Property, Competition and the Internet

July 25, 2012

Chairman Goodlatte, Ranking Member Watt and members of the Subcommittee, I appreciate the opportunity to appear before you to discuss cloud computing and the opportunities and challenges presented by this technology. My name is Daniel Castro. I am a senior analyst at the Information Technology and Innovation Foundation (ITIF). ITIF is a nonpartisan research and educational institute whose mission is to formulate and promote public policies to advance technological innovation and productivity.

In my testimony today, I would like to provide an overview of some of the benefits of cloud computing and then focus my remarks on two important principles for cloud computing: 1) creating "cloud-neutral" policies and 2) addressing anti-competitive foreign practices that challenge the dominance of cloud computing service providers in the United States.

An Overview of Cloud Computing Technology

Cloud computing refers to the growing practice of selling IT as a service that is delivered over the Internet. The most common forms of cloud computing include software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).

Software as a service (SaaS) is widely used by Internet users in the United States, such as to access web-based email or to share documents online. Users can access these applications online through a web browser on a PC or mobile device, rather than through software installed and run on a local desktop or server. Many of the most popular cloud-based applications are business productivity tools such as email (e.g., Gmail, Hotmail), online productivity software (e.g., Google Docs, Microsoft Office 365), conferencing services (e.g., Microsoft LiveMeeting, WebEx), and customer relationship management software (e.g., Salesforce).Using SaaS, customers can access software on-demand and pay for it on a metered basis, such as based on the level of usage or the number of users. Alternatively, there are many applications available at no-cost to users, and many of these are supported by ad-revenue.

Platform as a service (PaaS) allows users to rent virtualized software development or production environments ("platforms") to run their own applications or services. Organizations use PaaS to rapidly and efficiently develop and deploy new applications without having to invest in expensive hardware or software, or manage complex networking and computing infrastructure. PaaS can automate many complicated administrative technical functions, such as creating backups or test environments, and allow organizations to focus their resources on product development. PaaS also allows organizations to more easily scale up or down a computing environment to meet their computing needs for a particular application. For example,

Google App Engine allows developers to create and run Web applications that run on top of a custom Google platform and uses Google's computing resources.

Infrastructure as a service (IaaS) gives organizations of any size access to secure, enterprise-class computing infrastructure that can be efficiently managed and scaled to meet different needs. This allows companies to purchase computing resources on a metered basis, much like they would purchase electricity, water or any other utility. An example of IaaS is cloud storage, which provides users access to scalable online storage. Other IaaS approaches offer pay-as-you-go pricing for computing, data transfers and content distribution networks.

Cloud computing can be deployed in one of at least four different configurations: a private cloud, a community cloud, a public cloud, and a hybrid cloud. A private cloud is used exclusively by one organization with multiple business units and may be deployed either on-site or off-site. A community cloud is used exclusively by a specific group of organizations, often those sharing similar business interests or goals. For example, a community cloud may be provisioned for a group of federal agencies. In contrast to a private or community cloud, a public cloud is available for use by the general public. Lastly, a hybrid cloud refers to deploying an application or service across cloud computing infrastructure spanning two or more configurations (private, community, and public).[1]

Cloud computing has profoundly changed the economics of IT investments. In the previous model of computing, an organization would estimate how much computing power it needed, and then purchase the number of servers required to meet its peak needs. Most of the time, however, these computing resources would be underutilized. In addition, if an

organization's needs exceeded its estimates, the organization would have to scramble to purchase and bring online more servers.

Cloud computing eliminates many of these challenges. It creates a more flexible environment that allows organizations to "rent" computing power on an as-needed basis—an organization can scale up or down its IT usage according to demand. Organizations also benefit from the agility that cloud computing offers them as they have no long-term commitments and no high-fixed costs. Government agencies, for example, can better align cost with use by only paying for their actual use of IT resources, rather than having to overbuild capacity based on potential demand. This agility also allows organizations to easily upgrade their applications as they can change platforms simply by switching cloud providers. This flexibility is also useful for start-ups as it enables them to focus on building applications and services rather than on building a costly IT infrastructure. The concepts behind cloud computing—on-demand, scalable and pay-per-use—make it ideal for applications that have variable demand for resources or need to be scalable.

Cloud computing will involve significant changes in IT infrastructure for businesses in the coming years. For example, Gartner estimates that by next year sixty percent of server workloads will be virtualized.[2] Similarly a McKinsey survey of 250 chief information officers (CIOs) of large companies across different industries found that they expect over two-thirds of corporate applications to be virtualized by 2014.[3] Virtualization cuts the cost of computing by up to 50 percent with savings gains from lower infrastructure operational costs. Not only are legacy applications being virtualized, new IT investments are predominantly in cloud computing. IDC estimates that 80 percent of new commercial applications deployed this year will be on cloud computing platforms.[4]

Cloud computing allows organizations of any size to focus on their core business and not their IT. Running data centers—buying, installing, operating, maintaining, and upgrading servers—is resource intensive. Organizations benefit from cloud computing because service providers can provide greater economies of scale, share resources across multiple customers, and provide higher levels of expertise in operating a secure, reliable, and energy efficient data center. In particular, cloud computing has been a boon to startups as it reduces their need for capital investments to build, run and maintain IT infrastructure. As the CEO of one cloud computing startup noted, "Cloud computing has done to hardware what open source has done to software."[5] The availability of low-cost cloud computing infrastructure allows startups to create products without having to make a heavy investment in IT infrastructure. Instead, they can scale to meet their user needs as they grow. Unlike existing firms, which must integrate cloud computing with legacy IT systems, startups can start fresh.[6]

Create Cloud-Neutral Policies

Every technology creates new challenges. While some concerns have been raised about cloud computing, especially those relating to security and privacy, there is no need to create cloud-specific regulations. For example, cloud computing does not reduce an organization's responsibility for protecting its data. Storing data in the cloud instead of on an organization's own local servers does not reduce or limit the liability of an organization for ensuring the privacy of its data. An organization responsible for ensuring the privacy of its customer's data could be held liable for a breach of privacy regardless of if it occurs in the cloud or on its own local server. Questions of responsibility for ensuring the privacy of data between the organization who owns the data and the cloud computing service provider should be resolved through contract law. This means that organizations should be clear about the terms of service they receive from cloud

providers to ensure that they obtain the level of service they require. Consumers storing data in the cloud should also be clear about the terms of service and privacy policy offered by a service provider before storing their sensitive data online. Transparency is thus essential in cloud computing to ensure the market rewards good providers and penalizes bad ones.

Some concerns have also been raised about the privacy of data stored in the cloud and the legal regime governing it. In particular countries, especially some European countries, have argued that the Patriot Act gives the U.S. government more access to data stored by cloud computing service providers based in the United States than other governments have for cloud computing providers in their jurisdictions. While this is untrue, foreign competitors use this common misperception to seek an advantage over U.S.-based cloud computing service providers. As documented in a recent white paper by Hogan Lovells "it is incorrect to assume that the United States government's access to data in the Cloud is greater than that of other advanced economies."[7] In fact, the United States actually has more legal protections for some data stored in the cloud than other countries. For example, the United States has more restrictions on the voluntary disclosure of data stored in the cloud to government officials than in countries like Australia and Canada.[8] In addition, the existence of Mutual Legal Assistance Treaties (MLATs) between many countries means that many governments have the ability to obtain data stored outside of their jurisdiction.

Policymakers will eventually need to more thoroughly address the complex issues that come into play when data subjects, data owners, and service providers are under different legal jurisdictions and face conflicting regulations. These issues are not unique to cloud computing, but addressing these challenges will help simplify the regulatory complexity of using this technology. Meaningfully addressing jurisdictional issues may eventually require countries to

come to agreement on questions of jurisdiction or standardize some data practices. Alternatively, advances in technology that allow data policies to be bundled with data, and ensure that these policies are enforced, may also eventually help address some of the jurisdictional conflicts relating to cloud computing.

There has been some debate about the security of data stored in the cloud. Some people have argued that large amounts of data in the cloud represent an attractive target for hackers and thus data in the cloud is more at risk than data stored elsewhere. However, arguing that data in the cloud is more at risk because "there is more of it" is like arguing that because banks hold a large amount of money, and thus are an attractive target for bank robbers, people should not keep their money in banks. The fact is that for most individuals (and companies) money in a bank is safer than money under a mattress, and the same is true in the cloud. The reason for this is simple: because of their targeted focus and advantages in scale, cloud computing companies are able to develop expertise in secure computing that other companies cannot easily match. While cloud computing does not guarantee security, and organizations should investigate the terms of service and security practices of any particular service provider, the net result of a shift towards greater use of cloud computing in the United States will likely be a decrease in the overall security risk profile for many U.S. companies. In particular, this is true for small and mid-sized organizations that lack the required resources and expertise to implement a strong security program. Cloud computing represents an opportunity for these organizations to get better data security at affordable prices.

Creating "cloud-neutral" policies will require some changes to ensure that laws and regulations do not favor or disfavor cloud computing. One important step Congress can take in this direction is to update the laws that govern the electronic surveillance of data. The Electronic

Communications Privacy Act (ECPA) was enacted in 1986 and has not kept pace with the advancement of technology and the growth of cloud computing. As a result, there are different levels of legal protection afforded to the privacy of an individual's data based on where the data is stored and how long the data has been stored. This means that the right of the government to access a person's email may be different if it is stored on his or her PC versus if it is stored in the cloud. In the former case law enforcement might need a search warrant based on probable cause to review the data, but in the latter law enforcement would only need a subpoena.[9] However, the legal protections provided for an individual's private communications should not depend on the technology used to facilitate this communication. Consensus is forming that reform is needed in this area to protect Fourth Amendment rights.

Similarly policymakers should strengthen laws such as the Computer Fraud and Abuse Act (CFAA) which were written before cloud computing became widespread. Strengthening the CFAA would make it easier to prosecute criminals who hack into cloud computing services and establish penalties more in line with the impact of an attack. For example, CFAA should be changed to make penalties correspond to the number of accounts illegally accessed on an online service rather than limit them to the penalties for hacking into a single PC.[10] This will bring penalties more in line with the impact of such an attack.

Anti-Competitive Foreign Practices Threaten U.S. Cloud Computing

Not only have U.S. firms like Amazon, Rackspace, and Google pioneered cloud computing services, U.S. firms currently dominate the cloud computing market. As some of the primary providers of cloud computing technology, U.S. companies have tremendous potential for growth as cloud computing adoption increases worldwide. Worldwide adoption of cloud

computing is growing rapidly. On the low end, the International Data Corporation (IDC) estimates that the global market for cloud computing will grow to $56 billion by 2014. American Megatrends, Inc. (AMI) research predicts that the market for cloud computing will reach $100 billion by 2014 for small and medium businesses alone.[11] Forrester Research predicts that the market for cloud computing will grow from approximately $41 billion in 2011 to $241 billion in 2020.[12] Software as a service is expected to make up the bulk of this market at approximately $133 billion in 2020 worldwide.[13] IDC estimates that spending on cloud computing services will generate almost 14 million jobs worldwide between 2011 and 2015, including over 1 million jobs in the United States.[14]

Although U.S. firms are the leading providers of cloud computing services, other countries are aggressively challenging U.S. leadership in this market. For example, in April 2012 the French government announced it was funding one-third of a €225 million joint venture with two French telecom and technology companies, Orange Telecom and Thales, to create a new cloud computing company. This company will provide processing, storage, and bandwidth cloud computing services to French and European companies.[15] In May 2012, the French government announced a second joint venture of equal value to fund another company with SFR and Bull that will also provide cloud computing services.[16] China is similarly competing to create an internationally competitive domestic cloud computing industry. The Beijing government built a 7,800 square meter complex dubbed "Cloud Valley" and offers cloud computing companies tax-breaks and low-cost office space to locate in Beijing. The Chinese government is also allowing some firms to apply for a direct Internet connection to bypass the country's censorship system and access foreign servers so that foreign companies can outsource IT services to China.[17]

While some state-based efforts to promote domestic industries are legitimate (or semi-legitimate), others are clearly not. Fair competition in the market is healthy, but policymakers should be vigilant about identifying mercantilist policies enacted by countries to intentionally disadvantage foreign competitors. In fact, "cloud mercantilism"—the adoption of a wide array of policies and restrictions focused on import substitution for cloud computing services—is an emerging threat to global trade in information technology. And what makes this problem more challenging is that many nations use the guise of privacy and security to defend what are at heart mercantilist policies.

Some countries use data security and data privacy regulations to create geographic restrictions on where cloud computing service providers can store and process data. Restrictions on the cross-border flow of information diminish the ability of service providers to distribute data over a diverse geographic region to ensure redundancy and increase reliability, an important benefit of cloud computing. Other countries have policies that explicitly require cloud computing service providers to operate data centers domestically. Localization requirements have the effect of making cloud computing less efficient, since data center siting decisions must be made based on political mandates rather than technical or economic factors. Localization requirements also serve as a form of protectionism for domestic cloud computing providers since it may not be economically viable for a foreign competitor to build a new data center.

Examples of this type of behavior can be found in many countries. For example, Greece, Vietnam and Brunei have all passed laws which require data generated within the country to be stored on servers within the country.[18] Both the Norwegian and Danish Data Protection Authorities have issued rulings to prevent the use of cloud computing services when servers are not located domestically.[19] The Ministry of Communications and Information in Kazakhstan

issued an order to require that all .kz domain names operate on servers located within the country. The government later modified this order so that it only applied to new domains, rather than existing domains, however, this type of policy still unfairly discriminates against foreign providers.[20] China has implemented local data server requirements ostensibly to protect national security and control currency. Russia, Venezuela and Nigeria have all passed regulations requiring that IT infrastructure for payment processing be located domestically.[21] And similar types of laws are pending in other countries including Indonesia, Malaysia and Ukraine.

Other countries have flirted with various policies to advantage domestic firms or at least try to capture the economic benefits of constructing and operating a data center. For example, India has proposed a measure to require companies to locate their IT operations within the country so that law enforcement and national security agencies can obtain data stored on their servers.[22] And in Australia, legislation was proposed that would require that local data centers be used to store data in its electronic health record system.

The principles to combat these types of practices already exist. Under *The European Union-United States Trade Principles for Information and Communication Technology Services,* a set of principles agreed to by the Office of the U.S. Trade Representative and the European Commission, this type of behavior would be clearly prohibited. First, the principle on cross-border information flows states, "governments should not prevent service suppliers of other countries, or customers of those suppliers, from electronically transferring information internally or across borders, accessing publicly available information, or accessing their own information stored in other countries." Second, the principle on local infrastructure states, in part, "Governments should not require ICT service suppliers to use local infrastructure, or establish a local presence, as a condition of supplying services."[23]

In short, strong U.S. leadership is necessary to combat unfair trade practices that other nations are using to block foreign competitors in the rapidly growing cloud computing industry. First, the U.S. government should clearly and definitively state its opposition to local data server requirements and highlight instances of non-compliance by foreign governments. U.S.-based cloud computing service providers will have the most to lose if localization requirements become widespread. After all, the domestic market for cloud services is much smaller than the global market. Even today, Latin American and Asian companies are adopting cloud computing at higher rates than in the United States.[24]

Second, the U.S. government should affirm its intention to refrain from imposing its own local data center requirements. These policies may be tempting, especially for government procurement of cloud computing services. For example, when the City of Los Angeles negotiated to use Google Apps across its organization, it first required that Google create a special "Google Apps for Government" cloud service which restricted data from being stored outside of the United States.[25] While such requirements may at times serve short-term interests, they diminish the capacity of the United States to hold other countries accountable for similar forms of protectionism. The United States should avoid these types of policies otherwise it risks losing credibility on the international stage. The long-term goal of the U.S. government should be to work towards eliminating geographic restrictions on cross-border flow of data.

At the same time, if the United States is going to seek the moral high ground on free trade in cloud services, it will have to amend ECPA as described above and ensure that government policies do not treat cloud computing differently than any other information technology.

Thank you for the opportunity to share with you my thoughts on cloud computing. I look forward to answering any questions you have.

Endnotes

---

1. Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing," SP 800-145, National Institute of Standards and Technology, September 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
2. Ryan Nichols, "Cloud computing by the numbers."
3. Prashant Gandhi, Gary Moe and Kara Sprague, "Where the cloud is likely to grow," McKinsey Global Institute, 2012.
4. Derrick Harris, "It's cloud prediction time," GigaOm, December 1, 2011, http://gigaom.com/cloud/its-cloud-prediction-time-idc-gartner-and-i-weigh-in/.
5. Christopher Calnan, "Cloud computing bursting on the corporate scene", Mass High Tech, August 1, 2008, http://www.masshightech.com/stories/2008/07/28/weekly8-Cloud-computing-bursting-on-the-corporate-scene-.html.
6. Jonathan Boutelle, "How Cloud Computing Impacts the Cash Needs of Startups," Gigaom, August 16, 2010, http://gigaom.com/cloud/how-computing-impacts-the-cash-needs-of-startups/.
7. Winston Maxwell and Christopher Wolf, "A Global Reality: Government Access to Data in the Cloud," May 23, 2012, http://www.hoganlovells.com/files/Publication/80a807f2-c619-41dc-98c4-e6a7b5f6c5f8/Presentation/PublicationAttachment/0fc74c1d-4dc0-4c1c-9abc-eb50ae5679c4/Hogan%20Lovells%20White%20paper%20-%20Government%20access%20to%20data%20in%20the%20cloud.pdf.
8. Ibid.
9. For more on this issue, see the Digital Due Process Coalition, www.digitalducprocess.org.
10. See similar proposal in "Building Confidence in the Cloud: A Proposal for Industry and Government Action to Advance Cloud Computing," Microsoft, January 2010, http://www.microsoft.com/presspass/presskits/cloudpolicy/.
11. Ryan Nichols, "Cloud computing by the numbers: what do all the statistics mean," ComputerWorld, August 31, 2010, http://blogs.computerworld.com/16863/cloud_computing_by_the_numbers_what_do_all_the_statistics_mean.
12. "Cloud computing market: $241 billion in 2020," ZDNet, April 22, 2011, http://www.zdnet.com/blog/btl/cloud-computing-market-241-billion-in-2020/47702.
13. Ibid.
14. "Cloud Computing to Create 14 Million New Jobs by 2015," Microsoft News Center, March 5, 2012, http://www.microsoft.com/en-us/news/features/2012/mar12/03-05CloudComputingJobs.aspx.
15. "Orange and Thales welcome French State support for their joint project Andromède," Press release, April 20, 2012 http://www.thalesgroup.com/Press_Releases/Markets/Security/2012/20120420_DSC_Orange_and_Thales_welcome_French_State_support_for_their_joint_project_Androm%C3%A8de/.
16. "Vivendi's SFT and Bull Form Cloud Computing Company, Echos Says," Bloomberg, May 10, 2012, http://www.bloomberg.com/news/2012-05-10/vivendi-s-sfr-and-bull-form-cloud-computing-company-echos-says.html.
17. "Beijing hopes to dominate cloud computing with 'Cloud Valley,'" Smart Planet, December 16, 2011, http://www.smartplanet.com/blog/global-observer/beijing-hopes-to-dominate-cloud-computing-with-8220cloud-valley-8221/1313.
18. "Promoting Economic Growth through Smart Global Information Technology Policy," Business Roundtable, June 2012, http://mercatorxxi.com/merc/wp-content/uploads/2009/07/Global-IT-Policy-Paper-final.pdf.
19. See for example, "Processing of sensitive personal data in a cloud solution," February 3, 2011, http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution/ and "Will Not Let Norwegian Enterprises use Google Apps," January 25, 2012, http://datatilsynet.no/English/Publications/Will-not-let-Norwegian-enterprises-of-Google-Apps/.
20. "Changes to the Open Internet in Kazakhstan," Google Blog, June 7, 2011, http://googleblog.blogspot.com/2011/06/changes-to-open-internet-in-kazakhstan.html.

21. Ibid.
22. "Promoting Economic Growth through Smart Global Information Technology Policy," Business Roundtable, June 2012, http://mercatorxxi.com/merc/wp-content/uploads/2009/07/Global-IT-Policy-Paper-final.pdf.
23. "European Union-United States Trade Principles for Information and Communication Technology Services," April 4, 2011, http://ec.europa.eu/information_society/activities/internationalrel/docs/eu-us-tradeprinciples.pdf.
24. "The State of Adoption of Cloud Applications," Tata Consultancy Services, March 26, 2012, http://sites.tcs.com/cloudstudy/the-state-of-adoption-of-cloud-applications#.UAyxd7RfE4m.
25. An online help page for Google Apps for Government currently states that "Customer email and calendar data is stored only in facilities in the continental United States (CONUS)." Source: "Google Apps for Government," Google.com, n.d., http://support.google.com/a/bin/answer.py?hl=en&answer=174120 (accessed July 22, 2012).

Mr. GOODLATTE. The Chair is going to diverge from regular order because the gentleman from North Carolina has some other obligations, and we want to recognize him first to ask his question. So we will turn now to him.

Mr. WATT. I thank you, Mr. Chairman, and I thank you for accommodating my schedule. Unfortunately, I have got something that has started, and I need to be at immediately. But I did not want to miss the testimony or miss the opportunity to ask questions.

All of the testimony was very interesting and raises some very, very interesting issues. It seems to be unanimity on the question of cloud neutrality. I take it everybody is in agreement on that.

That means, I take it, that the same rules that apply to things outside the cloud should apply to things inside the cloud. Would that be a fair definition of cloud neutrality?

Mr. CASTRO. Yes, I do think that is a fair definition.

Mr. WATT. Okay. So but then you raise some interesting questions which, in essence, brings us back to a lot of the same issues

that we have been dealing with outside the cloud—protection of personal security, personal information for consumers, an issue outside the cloud, protection against trolls suing each other, although the owners of patents are suing each other regularly, which is a big problem, protection against piracy, which Mr. Holleyman raised in the context of the cloud, I presume to protect programs and what have you. But that is not unique to programs. Piracy is a problem.

And I do not want this to devolve into another question of how we protect ourselves against piracy, but it does raise the question of whether in light of the failure of our Committee to be able to deal with that effectively and the withdrawal of the proposal that was on the table, whether any affirmative steps are being made by the industry to address piracy either in the cloud or outside the cloud. If you are going to have a neutral cloud neutrality and you have got problems outside the cloud, then we have got to commit ourselves to working on the problems outside the cloud so that when we adopt the principle of cloud neutrality, those same principles will protect us inside the cloud.

So is anybody making any progress in the sector? You all obviously are all involved in this SOPA thing on one side or the other. We are not here to recreate that debate today. I just want to see whether you all think any progress is being made because if we are going to transport that issue to the cloud, we are going to have cloud neutrality, I think we got to deal with it. So, Mr. Holleyman?

Mr. HOLLEYMAN. Mr. Watt, thank you for the observation and question. The point which I want to make clearly about piracy in the cloud is there was a common myth, and candidly, I probably believed this myth as recently as 2 years ago, that software piracy goes away when software is used in a cloud context, and that where you actually have piracy is with the physical media, but that when you shift it to the cloud, you do not have the problem of piracy. And, in fact, what we found is that the piracy evolves.

I do think you will have less software piracy in a cloud context. We identified at least four ways in which it can occur, one of which will occur when unscrupulous hosters—fortunately, there are none that I know of at this point, but they may be ones outside elsewhere——

Mr. WATT. All right. You are identifying a set of problems in the cloud that are unique to the cloud, and I want to deal with. But that was not really my question.

Mr. HOLLEYMAN. Okay.

Mr. WATT. And I am running out of time.

Mr. HOLLEYMAN. I think your question—if I understand your question correctly, it was saying that some of the problems that we currently see are simply going to be transferred into an environment in the cloud. So what we need is effective tools to deal with those, and that is going to require self-help by industry. And that is also going to require appropriate use of law enforcement resources when the piracy can be identified, whether it is in the cloud or outside the cloud.

Mr. WATT. Well, my question was whether we are making any progress toward solving this problem outside the cloud or in the cloud. I guess that is the baseline question I am asking.

Mr. HOLLEYMAN. Yeah, I think we are making some progress outside the cloud where piracy is bigger in reducing levels of piracy. I think we have seen some good cases the Justice Department has brought that have been helpful. We bring about 10,000 cases a year. We are seeing piracy rates for software come down. What we have to make sure is that the tools that we need can continue to work in a cloud-based environment.

Mr. WATT. I would just open up one other area of inquiry. I know my time——

Mr. GOODLATTE. Without objection, the gentleman is recognized for an additional minute.

Mr. WATT. My time has expired, because it seems to me that this debate about whether we protect ourselves against other countries putting up barriers that allow hosting only in their countries is similar to this question of whether we do not prohibit call centers from going offshore.

The question is, how do we protect ourselves, how do we protect our own consumers' information without those kinds of barriers in our own country? And if we put them up in our own country, does that not incentivize other countries to put them up there? The same thing with national security concerns. If we are allowing our national security apparatus access to information in the cloud, would it not be a legitimate concern for other countries to be concerned about the extent to which our national security apparatus would have access to their information in the cloud?

I am not looking for answers necessarily to all of these questions, but it just seems to me from my simplistic mind that if we are setting up a set of neutral standards internationally and we are trying to get people to play by those rules, we have to anticipate that we have got our own set of issues we must deal with domestically before we can start fussing at everybody internationally. Am I off on the wrong cloud here, or do you all agree with what I am saying?

Mr. HOLLEYMAN. I will start by saying, hey, look, I think we need to do both simultaneously. I mean, there are some gaps in U.S. law that we think need to be resolved, like the need for ECPA reform that would ensure some greater levels of privacy for data that is stored in the cloud. And that would be an important signal for other countries.

And, secondly, we have to be aggressive in making sure, as one of my colleagues said, that we do not put rules in place that require all data on all U.S. citizens in all contexts to be held in the U.S. We do not require that now. There are some people who would like to do that, but if we did it, it would be a signal to every other country that they could do the same. So we have to live by that openness, but know that there are appropriate privacy and security regimes that will protect appropriate levels of data for U.S. citizens, wherever it's hosted.

Mr. WATT. Mr. Chairman, I appreciate your accommodating my schedule. I wish I could stay for another round of questioning because really I came with the intention of talking more about competition in the cloud, and I did not ask a single question about competition.

Mr. GOODLATTE. If you would submit your questions for the record, we would be happy to submit them to all the witnesses and ask them to respond.

And we appreciate the gentleman's participation. And the Chair now recognizes the gentleman from Texas, Chairman Smith for 5 minutes.

Mr. SMITH. Thank you, Mr. Chairman. I would like to try to see if I can squeeze in questions on the subject of patent trolls, privacy security, and foreign countries.

Let me direct my first question to Mr. Freeman. You and I have talked about this subject, and I have talked with two others within Rackspace on the problem of patent trolls, and the frivolous lawsuits they file, and the cost to the company and to other companies across America.

I think we are aware of the problem, though if you want to discuss it in greater detail, you are welcome to. But what do you think are some of the solutions to this almost exponential growth in lawsuits, litigation derived from these patent trolls?

Mr. FREEMAN. Thank you, Congressman. I think two key mechanisms that limit the incentives that patent trolls have to bring actions for profit without practicing their invention or practicing the patent. One approach along those lines is to limit the potential reward from litigation to the actual value of the license or that the troll are acquiring entity paid for a patent if it is not also practicing the patent. That is a case where the patent troll is essentially not being harmed by the practice of the invention by another entity, so it should not essentially get an ill-gotten gain simply as a result of holding onto a patent in an attempt to block innovation.

Another mechanism is to shift toward a framework where legal costs and responsibilities are borne more equitably between the two parties. A loser pays a price has been floated, and there are some interesting potential reforms along those lines. They can make it so that a patent troll has a lot or a litigator has a lot on the line when they file a claim for an infringement action.

Mr. SMITH. Okay. Good suggestions in regard to the first. I think we would have to probably be careful so that we would not apply such a reform too broadly. You cannot say it is illegal for someone to hold a patent just because they are not using it. But I understand the thrust of your reform, and I agree with that.

Mr. Holleyman, on the subject of privacy, what are some of the privacy issues involved with cloud computing that we need to be aware of? And you just started getting into that a little bit I think in response to the question from Mr. Watt.

Mr. HOLLEYMAN. Right. On the issue of privacy or piracy?

Mr. SMITH. Privacy.

Mr. HOLLEYMAN. Privacy. Well, look, I think on the issue of privacy, one of the single biggest issues is going to be how we work in the context of the European Union, which is moving to adopt a data privacy regulation that will be unlike a directive. This will be mandatory across all 27 member states. There is sort of an 18- to 24-month process in which that is happening, and that is going to require a regular dialogue with U.S. government, both Administration and U.S. Members of Congress, because at the end of the day, we have to have a regime that preserves the safe harbor, provisions

that currently have been negotiated between the U.S. and the EU so that data can be exchanged appropriately across borders. And that we also have to ensure that the Europeans do not adopt a privacy regime that is so restrictive that will have a de facto effect of blocking access by U.S. companies.

Mr. SMITH. And as you say, we have seen some signs of that already I think.

Mr. HOLLEYMAN. Absolutely.

Mr. SMITH. Thank you. Mr. Chenok, I want to ask you about security issues involved with cloud computing. You touched on them a minute ago, but can you elaborate?

Mr. CHENOK. Yes, thank you for your question. Security in the cloud is——

Mr. SMITH. Is your mic on?

Mr. CHENOK. Yes, I will do that. Thank you for your question, Chairman Smith. Security in the cloud is not dissimilar to how security is handled in other forms of technology. You could imagine a cloud with very strong security protections built into the system—lots of surveillance of the Internet traffic coming out of the cloud, immediate warnings to the operators of the system that then go out to the users of the cloud if there is an incident. Similarly, you could imagine those same kinds of protections being built into a well-constructed system that is a more traditional system, let us say a client server system or another type of computing system.

So security issues in the cloud in some ways can be built very well or not. And the key is to incentivize, and for companies like ourselves that are here with you today to understand how to build security into solutions that we develop for the cloud from the beginning so that customers of ours—consumers, businesses, and governments—have confidence that the solutions that we provide and the solutions that are discussed in the context of government to government discussions are secure and private.

The other point I would make, just reiterating what was in the testimony, is that the cloud itself can provide for a much more rapid response if there is a security incident that comes in. If you are in a traditional environment with lots of different servers in different places and different people worrying about those, and a computer security incident occurs in a patch to fix the incident is delivered, it is often delivered essentially manually from place to place and person to person. With the cloud, you can deliver that patch automatically, instantaneously, and the problem is rectified immediately.

Mr. SMITH. Okay. Thank you, Mr. Chenok. I am out of time. Mr. Castro, I just want to thank you for answering my question a minute ago in your opening statement about the threat of foreign countries and what our government should do. You were very specific. I hope the Administration will listen.

Thank you, Mr. Chairman.

Mr. GOODLATTE. I thank the gentleman. The gentleman from New York, Mr. Nadler, is recognized for 5 minutes.

Mr. NADLER. I thank the gentleman.

Mr. Castro, a key guiding principle articulated by several company witnesses at one of our prior hearings held in September 2010 when I was Chairman of the Constitution Subcommittee was the

desire for technology neutral or cloud neutral, as it has been described today, standards for government access to communications under the Electronic Communications Privacy Act, ECPA. This would mean that with regard to government access to content communications stored in the cloud, communications stored in the cloud would be treated the same as communications stored locally by a customer.

If a primary goal for ECPA reform is establishing clear and consistent standards, it does seem that this would be essential. Do you agree?

Mr. CASTRO. I do agree.

Mr. NADLER. Anybody else agree or disagree on that? Everybody agrees that we should have the same standards for government access to material stored in the cloud as for government access stored on your laptop.

And, Mr. Holleyman and Mr. Chenok, the principle we are discussing, that of cloud or technology neutrality, is a core principle of the Digital Due Process coalition. DDP takes the position that "Government access to content and communications should require a search warrant issued based on a showing of probable cause, regardless of the age of the communications, the means or status of their storage, or the provider's access or use of the communications in its normal business operations."

This technology-neutral standard adopts the current standard for communication stored by an individual locally for the communication stored in the cloud. IBM and BSA are members of the Digital Due Process coalition, so I presume your companies would support a bill adopting this standard. Would you agree with that or comment on it, Mr. Holleyman first.

Mr. HOLLEYMAN. BSA is a member of the Digital Due Process coalition, and we support their recommendations.

Mr. CHENOK. And IBM is a member of the Digital Due Process coalition and support it, yes.

Mr. NADLER. So you would agree that the standard should be a due process standard, a search warrant based on a showing of probable cause, regardless of age. We have in ECPA now these different standards based on whether it is longer than 180 days or less than 180 days based on assumptions 25 years ago that if you had it on your computer or on somebody else's computer for more than 180 days, obviously you did not care about it. You did not care about your privacy. Does everybody agree that that logic is no longer the case?

Everybody seems to agree?

Mr. HOLLEYMAN. Mr. Nadler, I agree with that logic, and, again, we are part of that coalition and support those recommendations. I would actually like to follow up with some additional detail for the record for your question.

Mr. CHENOK. I would join Mr. Holleyman in following up.

Mr. NADLER. I thank you. I yield back.

Mr. GOODLATTE. I thank the gentleman. The gentleman from Pennsylvania, Mr. Marino, is recognized for 5 minutes.

Mr. MARINO. Thank you, Chairman.

Good afternoon, gentleman. Thank you for being here. As a former prosecutor, I believe that for every action there is an equal

and opposite reaction. So with that said, we in America, we are very good at developing technology, the best in the world I think. But nevertheless, we fall short worldwide of anticipating the downside of our advancements and our technology. And pursuant to our topic today, the clouding issue, I am going to ask each of you to take a moment and perhaps predict what you see the downside of the technology that we are achieving today concerning clouding. Do you understand my question? Mr. Holleyman?

Mr. HOLLEYMAN. Look, I think the biggest downside I see is that there are going to be a lot of changes in the economy that result, as you move to using this new technology, which means that the nature of some jobs will change, the nature of how information is stored has changed. But as I began with the IDC report, there is also a huge value add to the economy, as much as a trillion dollars in new growth, not just in technology, but across all sectors because of cloud-enabled innovation.

Mr. MARINO. Okay. Mr. Freeman, do you have a comment?

Mr. FREEMAN. I think I echo those thoughts. There is going to be an economically disruptive effect as the amount of data that is available and information about individuals' consumption behaviors is magnified exponentially. If there is not an alignment of the legal principles and the legal system applicable to types of data, regardless of whether they are stored in the cloud or locally, I think that is going to pose a big challenge and potentially be disruptive to continue cloud innovation.

Mr. MARINO. Thank you. Mr. Chenok?

Mr. CHENOK. Thank you, Congressman Marino, for your question. I think two points. One, if not implemented well as with any technology, cloud can increase issues involved in how a technology is placed in a work location or used by a user. So the concern would be address cloud's implementation and make sure that it is done in a manner that addresses some of the issues that we have discussed here today earlier with regard to location mandates and open standards to make sure that those types of policy choices are built into the implementation. Without that, you could get some unintended effects.

And also misperceptions. Some of us have talked this morning about certain beliefs about the cloud that are not necessarily true in fact, but color how people come to it and color the uptake in terms of use of the cloud. And so thinking of fact-based, I think, is very important.

Mr. MARINO. Thank you. Mr. Castro, do you have a thought?

Mr. CASTRO. Yes. You know, I think cloud computing technology is disruptive businesses and organizations and government in very positive ways. But it is also, of course, there is a duality to technology, and it can be used for negative purposes as well. So just as we see legal businesses becoming more productive and doing more with this technology, we can also see that taken up by illegal activity to be more productive. And obviously that is a very bad thing.

Mr. MARINO. A good segue into my next question concerning the illegality of it and the potential of those outside. It should not be in a particular area garnering the information, penetrating the system. How about our security end of the thing, anyone?

Mr. HOLLEYMAN. In a cloud context, you need to look at kind of the access controls and how it is secured. I mean, the cloud, if configured properly, can be a much more secure environment than the highly distributed environment we have today where people leave laptops or they leave their thumb drive. And so if done properly, the cloud can be a net positive.

Mr. MARINO. Well, let us take it a step further, and I am going to use an example. Years ago in law enforcement, we develop a basic walkie-talkie where law enforcement can communicate with one another. But then quickly, there was developed a scanner where we could—where the criminals could hear that we were coming after them. So how do we prevent that? Has that been taking into consideration at this point? I know we're anxious to put this all together, but are we thinking of the ramifications and the technology that can really counter what we intend to do?

Mr. CHENOK. So, Congressman Marino, there are technical protections that can be built into data in transit that can be established and assigned to the cloud in terms of understanding how information is moving and whether there is interception of that information while it is moving, and can very quickly spot when somebody is trying to penetrate a system or penetrate a set of information resources that are moving along, and then quickly identify how to resolve that situation.

And continuing to build those technologies in and designing the system properly from the front will help to address those types of risks.

Mr. MARINO. And, Mr. Castro, I am going to flip a question to you. I am running short of time here. How many entities within when I send my e-mail to whoever is receiving it are going to have access that information within that cloud?

Mr. CASTRO. In theory, you could have just one. You know, you could have just the one actual provider, depending on how the cloud computing environment is set up. Ideally, you have it virtualized in a way that the data is actually segmented in ways that other providers that might be offering services would not actually have access to your specific data.

Mr. MARINO. I see my time has run out. Thank you, gentleman. My daughter is going to be proud of me because I was talking about the cloud system today. [Laughter.]

Thank you. Thank you, Chairman. I yield back.

Mr. GOODLATTE. Does she think most days you have your head in the clouds? [Laughter.]

Like my teenagers did when they were that age? The Chair is pleased to recognize the gentlewoman from California, Ms. Lofgren, for 5 minutes.

Ms. LOFGREN. Thank you, Mr. Chairman. My apologies for being late. I had a competing meeting. But I do think that this is a very important discussion. I understand Mr. Nadler raised the issue that I have also been working on, the need to update ECPA for our current technology times. It has been a long time. And there are certainly privacy issues that need to be addressed, and certainly some of the assumptions that Americans have about the privacy afforded their digital data is not, in fact, adhered to under the legal

standards. And so that is something that I hope to help address as time goes on.

I am wondering, in terms of as we deploy throughout the world, whether there are issues that we also need to address on standard setting for interoperability and portability of data when it comes to cloud computing, something I have not heard discussed at all, and yet I think it is pretty obviously something that needs to at least be attended to. Am I mis-advised to be concerned about that?

Mr. FREEMAN. I think that is very correct. I think there are two key types of portability that have to be considered. The portability of user data, you can rapidly see adverse effects if cloud data or user data is stored within a given provider, and users of businesses are essentially held hostage and unable to extract that data later.

Ms. LOFGREN. That is right.

Mr. FREEMAN. The other thing is the portability of applications, the services that essentially are the cloud. If a government agency or a business is too reliant on a single provider's proprietary infrastructure and may find itself unable to migrate out to either another provider in the case of a service issue or be left without an alternative solution in the case of a service failure.

Ms. LOFGREN. I am interested as well—I think some of the security issues have been dealt with. But I think there is an overlap between, maybe for lack of a better word, security issues and interoperability. And I wanted to raise the issue of—and I will use the U.S. as an example. We recently took an action, we as the United States government, against a site alleged to be a big pirate site, Megaupload. But in a way, that is also cloud computing. I mean, it is not what we think of in the business world, but that is what it is.

Have you addressed the issue of governments aggressively enforcing property rights when it comes to cloud computing that then disadvantages other users? We have heard for example that why somebody would store their baby pictures on Megaupload, I do not know, but apparently some people did. And now their baby pictures are going to be toast.

Have we addressed that issue as a group that thinks about it, how we can protect innocent users when there are enforcement actions?

Mr. HOLLEYMAN. Ms. Lofgren, I am totally familiar with Megaupload case, and I know that there are some pending proceedings both at Justice and in the courts, of which I am not privy to——

Ms. LOFGREN. Right. I just use that as an example. You do not have to talk about that case.

Mr. HOLLEYMAN. Look, I think one of the questions is given the scope of some of what I would refer to as just, you know, storage facilities, and how to ensure that you have protection for the legitimate data that is stored, recognizing that you still need tools to be able to deal with the illegitimate data that may be stored or the hosting entity.

And I think it is going to take, you know, a balance of laws. What is important, though, is that you still have to have tools, both civil and criminal, that allow you to take action——

Ms. LOFGREN. Oh, I am not arguing that case. But nobody seems to feel any responsibility toward people who are completely innocent here. And there is no standards. There seems to be no interest or obligation to innocent bystanders to this action. I am wondering if there is not something that we ought to do to address that issue.

Mr. HOLLEYMAN. Again, I cannot suggest an answer to that. I think that is a legitimate question. It is a legitimate question you are asking. I mean, we had, as BSA, been engaged in a lot of notice and takedown activity with Megaupload, and there were certainly some illegal software that was part of that.

Ms. LOFGREN. Sure.

Mr. HOLLEYMAN. And there has now been, we both independently and obviously through Justice, have had some recourse. But I cannot go beyond that to talk about——

Ms. LOFGREN. Well, let us just use it as an example, not that——

Mr. GOODLATTE. Without objection, the gentlewoman is recognized for an additional minute.

Ms. LOFGREN. Thank you, Mr. Chairman. If any of the witnesses have a suggestion on whether we should not have some standards so that innocent bystanders, if you will, have some recourse and rights, I would be maybe off calendar eager to hear them.

Mr. FREEMAN. I would like to speak to that, if I may, Congresswoman. I think the key is an alignment of existing privacy and criminal standards with regards to search and access, regardless of the location or the nature of how data is stored.

You highlighted ECPA earlier, and e-mail is treated differently when I print it out and put it in my desk than it is when it is on my computer than it is when it is on Gmail server. That alignment, along with a bit of international consistency, I think will solve the problem for both businesses and consumer.

Megaupload is a case that, for example, highlights the use of mutual legal assistance treaties to create a coherent and enforceable regime. But if those standards are not consistent with regards to the data type, regardless of technology, and if they are not consistent internationally, there will be a lack of transparency and perceived lack of protection for users' data.

Mr. GOODLATTE. The time of the gentlewoman has expired.

Ms. LOFGREN. Thank you, Mr. Chairman.

Mr. GOODLATTE. And the Chair will recognize himself for questions.

Mr. Holleyman and Mr. Freeman, what are some of the more egregious market access issues that BSA or Rackspace or other businesses have found foreign countries engaging in against American cloud computing companies in the European Union or in countries like Canada, Australia, India, Japan, China? As I prepared this question, it seemed to have gotten longer. We will start with you, Mr. Holleyman.

Mr. HOLLEYMAN. Mr. Chairman, it is unfortunately an increasingly long list, as we pointed out in our report. I will give you two countries at opposite ends of the spectrum. China has a requirement that you must have a joint venture with a Chinese entity to provide a cloud service in China, and there is a condition of providing source code in conjunction with that. And China is no longer allowing joint ventures, and of course companies are rightly resist-

ing any source code disclosures. So effectively, you have a great wall that has been erected and continuing to be erected that is going to shut out companies in the China market.

On the opposite end of the spectrum, you have the concerns I see happening in Germany where German government officials are talking about the fact that all German data should be stored in Germany, both high sensitive and low sensitive and medium sensitive data, not only for the German government, but for German citizens. And then you have a marketing campaign by Deutsche Telecom, which is effectively a third owned by the German government, that is invoking the PATRIOT Act and citing the PATRIOT Act as a reason why customers should use Deutsche Telecom's hosting services over U.S. providers.

And so I think those are two ends of the spectrum, and we need to address those problems in both countries. And they are just an example of what we see elsewhere.

Mr. GOODLATTE. Does Deutsche Telecom still own T-Mobile? Is that the relationship there?

Mr. HOLLEYMAN. Well, my understanding is that they still do, but I am not the expert on that.

Mr. GOODLATTE. Following up on that very distressing point, having worked as hard as I have on the PATRIOT Act, what are some of the misconceptions that they are spreading about the PATRIOT Act, or data privacy policies in the United States in general that would help them steer business to Germany companies or other countries that may be doing the same thing?

Mr. FREEMAN. I can tell you at Rackspace, we commonly see almost occasionally absurd positioning of what the PATRIOT Act permits to the extent that it allows almost any U.S. government agency to, without notice or warrant, access any private data that is on a server contained within the United States. That sort of——

Mr. GOODLATTE. Well, that is totally false.

Mr. FREEMAN. That sort of fear, uncertainty, and doubt I think inform Canada's FOIPA law, which is a good example of a protectionist measure that excluded U.S. participation in the marketplace. Canada passed a patient privacy bill that prohibited the storage of any patient health information on any server located in the United States based on this sort of fear and uncertainty. Now I think it was more of a protectionist measure that has leveraged that type of fear. But our great concern is that we see the same types of positioning being touted in marketing campaigns such as in Germany and the rest of Europe.

Mr. GOODLATTE. So what do you do to counter that? Do you have a Rackspace Germany that is a separate entity with your cloud computing capabilities there, or what do you do?

Mr. FREEMAN. Thank you, Chairman. Even having a subsidiary entity these days is being targeted. Essentially, there is an approach that anyone who has either a server in the United States or is a subsidiary or joint venture with the U.S. company is becoming suspect.

Again, I think these are really pretenses for protectionist pressures, and that they are not based on legitimate understanding of the legal principles. I think the best way to deal with it is through education, and the establishment of international standards, and

clear statements from the U.S. government about how the PATRIOT Act works and how it is utilized and implemented.

I think we all are sort of aware that foreign countries all have access in certain circumstances to data for servers that are located on their soil.

Mr. GOODLATTE. I would argue most countries have far greater access to that data in their countries without the Bill of Rights that the United States Constitution provides for protection of U.S. citizens that would extend to anybody storing their data in the United States.

So what do you suspect we should do with regard to this in the sense that it is a trade issue, that it is a protectionist policy? Have any of you approached the U.S. Trade Representative to address this issue?

Mr. HOLLEYMAN. Chairman, I will give you a couple of answers. One is that the State Department has actually been very aggressive in raising this with other countries. Ambassador Riviere is leading that effort. There is a new myth busters document that State and Justice are working on to try to dispel the myths about the PATRIOT Act, and dispel the myth that somehow the U.S. has powers here that other countries have. And I think there has to be a bilateral, aggressive negotiation. And I also think that you see through USTR on efforts like the Trans-Pacific Partnership and building new trade agreements that deal with issues around cross-border data transfers that are related to, but an important complement to dispelling these myths about the PATRIOT Act.

Mr. GOODLATTE. Mr. Chenok, as more data moves to the cloud, where do you see the future of data analytics? What are some of the innovations that we can expect in this new field of technology?

Mr. CHENOK. Analytics is——

Mr. GOODLATTE. Put the microphone on again.

Mr. CHENOK. Analytics runs on a parallel track, Mr. Chairman, if you will, with the cloud. The cloud enables companies of all kinds and governments to understand information regardless of where it sits. Through the cloud, you can use technology to get to information more effectively and efficiently and at less cost. So it enables the type of analytics that can be done to really make decisions very quickly and rapidly based on data regardless of where it sits over an open cloud, without having to establish point to point agreements or computer interface exchanges that might take time and increase costs to achieve the same level of the data coming together to make an analytical decision. So the two are related and mutually reinforcing.

Mr. GOODLATTE. Thank you. Those are the questions that I have. Since the buzzer for the votes have not gone off yet, I will ask the gentleman from Pennsylvania or the gentlewoman from California if they have an additional question they would like to ask the panel of experts before we dismiss them. The gentlewoman from California.

Ms. LOFGREN. Mr. Chairman, thank you for that opportunity. There was some testimony on abusive patent litigation. And it is something I am concerned about, but I am not sure we have got the energy to wade back into patent reform. But I am wondering

if we could get some suggestions on how the Patent Office itself might make that situation a better one.

Mr. FREEMAN. Thank you, Congresswoman. I think it is difficult to approach it with the current regulatory authority of the Patent Office itself. I am reluctant to tell you that I have all of the solutions to the problem because it is really based on behavior——

Ms. LOFGREN. Well, join the club.

Mr. FREEMAN. Yeah. It is really based on the behavior of a set of entities who are exploiting a system that works well in many cases. And there is no need to throw out the baby with the bath water, so to speak, but I think sort of responsive action is necessary.

One area is particularly in regards to the development and increasing use of open source cloud software. The patent system does not work particularly well when it comes to collaborative open source projects because it really did envision more of a focus reward and innovation generating system.

Ms. LOFGREN. Well, we did have just recently some further discussion on standard setting in the patent system and how we might work with that. So, again, I am sorry I was unable to get here for all the testimony, but I do think that when you look at what, as the Chairman has said, certain countries are doing in terms of using tools to block market access, sometimes with legitimate concerns honestly about the lack of standards in American law. I mean, EPCA is one of them.

We have a lot of work to do in this area, and I am glad that we had this hearing, Mr. Chairman. And I think we will be working diligently in the coming months to address some of these issues. And I yield back.

Mr. GOODLATTE. I thank the gentlewoman. The gentleman from Pennsylvania does not appear to have any additional questions. So we will thank our witnesses for their excellent testimony today.

And without objection, all Members will have 5 legislative days to submit to the Chair additional written questions for the witnesses which we will forward and ask the witnesses to respond to as promptly as they can so that their answers may be made a part of the record.

Without objection, all Members will have 5 legislative days to submit any additional materials for inclusion in the record.

And with that, I again thank our witnesses. And the hearing is adjourned.

[Whereupon, at 1:25 p.m., the Subcommittee was adjourned.]

APPENDIX

Material Submitted for the Hearing Record



BUSINESS SOFTWARE ALLIANCE

Robert W. Holleyman, II
President and Chief Executive Officer

20 F Street, NW
Suite 800
Washington, DC 20001

p 202/872 5500
f 202/872 5501

WWW.BSA.ORG

August 15, 2012

The Honorable Jerrold Nadler
Subcommittee on Intellectual Property, Competition, and the Internet
Committee on the Judiciary
United States House of Representatives
2138 Rayburn House Office Building
Washington, DC 20515-6216

Re: Additional Information for the Record – "Cloud Computing: An Overview of the Technology and the Issues Facing American Innovators"

Dear Congressman Nadler:

I am writing here to follow up on your questions during the Subcommittee's recent hearing on "Cloud Computing: An Overview of the Technology and the Issues Facing American Innovators." As I indicated during my testimony, the Business Software Alliance (BSA) supports updates to the Electronic Communications Privacy Act (ECPA) in line with the principles of the Digital Due Process (DDP) coalition.

Specific to your questions on ECPA reform, you asked whether BSA would support: 1) "technology neutral or 'cloud neutral' ... standards for government access to communications under" ECPA; and 2) "a bill adopting this standard."

As I testified during the hearing, BSA would support such a "cloud neutral" approach to the standards for government access to electronic communications as proposed by the DDP coalition. BSA is a member of the coalition, which also includes privacy advocates, major companies, and think tanks. DDP was guided by the concept of technology and platform neutrality as it shaped is principles. As DDP defines this concept, it means that a "particular kind of information (for example, the content of private communications) should receive the same level of protection regardless of the technology, platform or business model used to create, communicate or store it."

In practice, using the concept of technology and platform neutrality to shape ECPA reform would ensure that cloud computing customers enjoy the same legal protections for their private documents as those individuals who store files on their own computers. Such reforms would have great benefits for consumers who take advantage of the enhanced security, flexibility and collaboration offered by cloud computing services. It would eliminate the confusing and conflicting standards and illogical distinctions that mark today's system. For example, the law today protects a document stored on a person's desktop computer with the warrant requirement of the Fourth Amendment. If the person saved that same document to an online storage service, however, it may not be subject to the warrant requirement under ECPA. This incongruity results from the tremendous advances in technology in the years since

ECPA was first adopted, and it serves only to undermine consumers' confidence in the technological paradigm that increasingly powers our economy.

Accordingly, and to your second question, BSA would support legislative efforts to update ECPA in line with the coalition's recommendations. BSA's endorsement of any such bill, however, would depend on the full range of issues implicated by the bill, including those that go beyond the recommendations of the coalition.

As a reminder, the Digital Due Process coalition's ECPA reform principles are as follows:

> **Overarching goal and guiding principle:** To simplify, clarify, and unify the ECPA standards, providing stronger privacy protections for communications and associated data in response to changes in technology and new services and usage patterns, while preserving the legal tools necessary for government agencies to enforce the laws, respond to emergency circumstances and protect the public.
>
> These principles would not change, and are subject to, the current definitions, exceptions, immunities and permissions in ECPA.
>
> - A governmental entity may require an entity covered by ECPA (a provider of wire or electronic communication service or a provider of remote computing service) to disclose communications that are not readily accessible to the public only with a search warrant issued based on a showing of probable cause, regardless of the age of the communications, the means or status of their storage or the provider's access to or use of the communications in its normal business operations.
>
> - A governmental entity may access, or may require a covered entity to provide, prospectively or retrospectively, location information regarding a mobile communications device only with a warrant issued based on a showing of probable cause.
>
> - A governmental entity may access, or may require a covered entity to provide, prospectively or in real time, dialed number information, email to and from information or other data currently covered by the authority for pen registers and trap and trace devices only after judicial review and a court finding that the governmental entity has made a showing at least as strong as the showing under [section] 2703(d) [of the Stored Communications Act[1], which was enacted as the second title of ECPA.[2]]

[1] *See* 18 U.S.C. § 2701-2711 (2012).
[2] See Electronic Communications Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in sections of 18 U.S.C.).

- Where the Stored Communications Act authorizes a subpoena to acquire information, a governmental entity may use such subpoenas only for information related to a specified account(s) or individual(s). All non-particularized requests must be subject to judicial approval.[3]

In line with my testimony, I also would like to commend you and Congressman Conyers for your recent introduction of H.R. 6339, the Electronic Communications Privacy Act Modernization Act of 2012. H.R. 6339 includes valuable elements that align with the Digital Due Process coalition recommendations, and it would make important updates to ECPA. We would need to review further with our members the elements of the bill that go beyond the coalition's recommendations, such as the provisions that would create new information sharing requirements. We applaud your efforts to update ECPA in order to bring it up to date with today's technology, and we look forward to working with you on this important legislation.

On behalf of BSA and all of our member companies, I want to thank you and the full membership of the Subcommittee on Intellectual Property, Competition and the Internet for your attention to the full range of policy matters relevant to cloud computing.

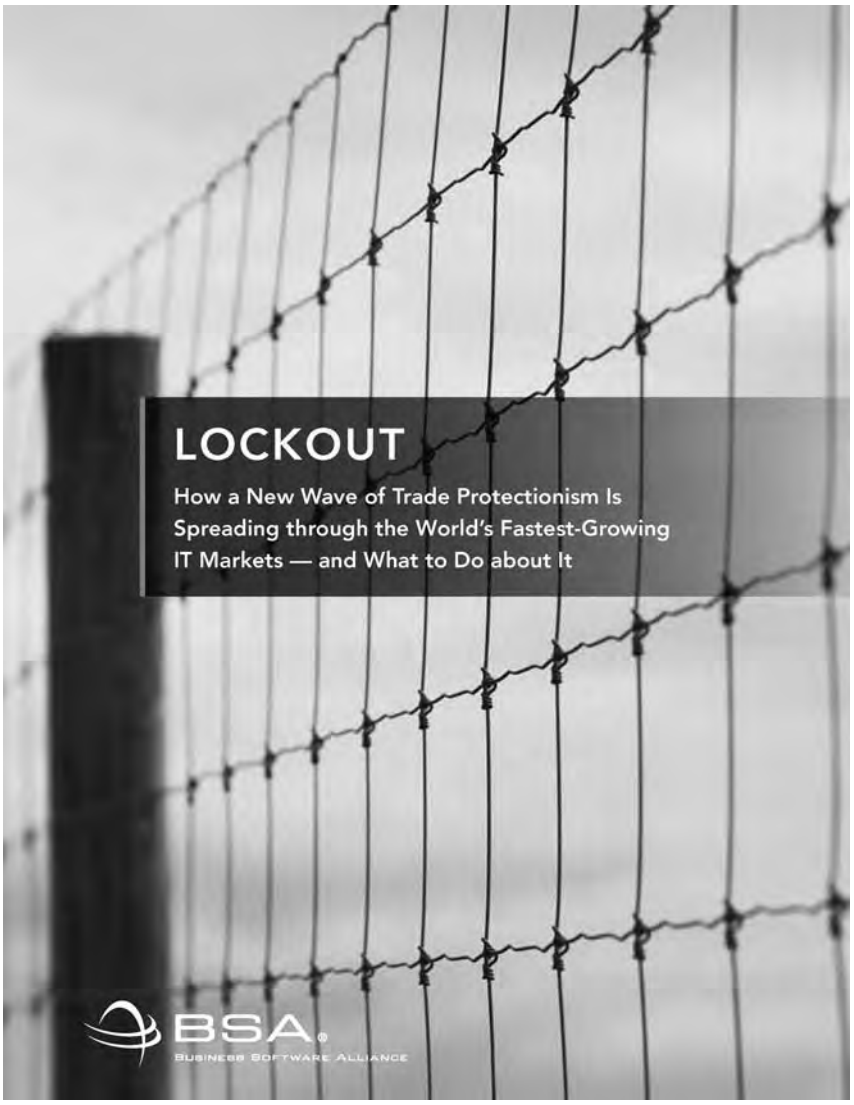
Sincerely,

Robert Holleyman

Robert W. Holleyman, II
President and CEO

[3] Digital Due Process coalition principles, available at http://digitaldueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163.

Supplemental Material submitted by Robert W. Holleyman, II, President & Chief Executive Officer, Business Software Alliance (BSA)



CONTENTS

Executive Summary 1

Confronting a New Generation of Market-Access Barriers 2

BARRIER ONE: Restrictions on Procurement by Government Agencies and State-Owned or State-Influenced Enterprises 4

CASE STUDY: Mandates for Procurement of Domestic Electronic Goods in India 4

CASE STUDY: Price Preferences for Procurement of Local Goods in Brazil 5

CASE STUDY: Central and State-Level Procurement Preferences in Indonesia 6

BARRIER TWO: Manipulation of Technology Standards 7

CASE STUDY: Restrictive Standards Policies and Practices in China 7

CASE STUDY: Unreasonable Terms for Standards-Essential Patents and Preferences for Indigenous Technology in India 8

BARRIER THREE: Overreaching Security-Related Regulations 9

CASE STUDY: Restrictions on the Procurement of Foreign IT Security Products in China 9

CASE STUDY: Burdensome Security Testing for IT Products in India 10

BARRIER FOUR: Regulatory Obstacles to Cloud Computing 10

CASE STUDY: Licensing Requirements Restricting Foreign Companies' Ability to Offer Cloud Services in China 11

CASE STUDY: Restrictions on Cross-Border Data Flows & Location Requirements for Data Centers in Indonesia and Vietnam 12

BARRIER FIVE: Persistent Tariffs 14

BSA Policy Recommendations 15

About BSA 18

Endnotes 20

Executive Summary

Many of the world's largest and fastest-growing emerging markets are erecting new trade barriers that discriminate against foreign information technology (IT) products and services. More troubling, these barriers — in China, India, Brazil, and elsewhere — are having a contagion effect, emboldening other emerging markets to impose protectionist measures of their own. The global scope of the problem poses immediate and long-term threats to the IT industry and the broader global economy. These threats cannot be overstated or ignored. Leading IT economies should press a concerted bilateral, multilateral, and regional effort to combat discriminatory trade barriers where they already exist and eradicate them before they spread further.

The IT industry is a critical driver of economic and job growth. Any barriers to IT sales and exports in major emerging markets therefore undermine the ability of IT firms to contribute to the global economy. Moreover, while many of the barriers erected by emerging markets are aimed at bolstering the growth of domestic IT sectors and these countries' economies more generally, protectionism can backfire over the long term. Denying these markets access to foreign goods, services, and investment that can be a catalyst to economic growth and innovation can impede the very goal these countries are trying to achieve.

The new generation of market-access barriers cropping up in emerging markets are numerous and not always as easy to identify as traditional trade barriers. That also makes it difficult to challenge them with traditional trade remedies alone.

Some of the major impediments that IT companies face — such as poor intellectual property (IP) protection and enforcement, and severe limitations on investment in new operations — plague other industry sectors, too. This report focuses on several categories of barriers that particularly hamper market access for IT goods and services, including:

1. **Restrictions on procurement by government agencies and state-owned or state-influenced enterprises.** These include mandates or preferences for domestically owned or produced products, for products utilizing a particular technology or business model, or for products whose intellectual property is owned or developed locally.
2. **Manipulation of technology standards** to bolster domestic firms and insulate them from foreign competition.
3. **Security-related regulations that limit market access for foreign information security and other IT products** by mandating the use of local products or imposing unreasonable testing or certification requirements.
4. **Regulatory obstacles to cloud computing** that unduly burden or discriminate against foreign firms by, for example, requiring suppliers offering cloud services to locate data centers in-country or by significantly restricting cross-border data flows.
5. **Tariff barriers** that persist because many key emerging markets have not joined the Information Technology Agreement (ITA), and the agreement does not cover important new categories of software and hardware.

The US, Europe, and other governments should urgently elevate these market-access concerns in bilateral, multilateral, and regional trade discussions. Eliminating IT-focused barriers will require updating World Trade Organization (WTO) frameworks, taking appropriate measures in new trade agreements such as the Trans-Pacific Partnership (TPP), and marshaling support for open markets in regional dialogues such as the Asia-Pacific Economic Cooperation (APEC) forum. In addition to employing current trade tools where appropriate, trade officials also should consider where robust new tools may be needed.

BSA offers the following action plan:

- **Press trading partners to adopt transparent, nondiscriminatory government procurement policies.**
- **Ensure that commercial procurement by state-owned or state-influenced enterprises is undertaken without government intrusion.**
- **Use trade agreements to establish rules that promote market-led technology standards.**
- **Establish clear rules allowing data to flow across international borders.**
- **Advocate for strengthened IP protection and enforcement, and oppose market-access restrictions based on the location of IP ownership or development.**
- **Enforce existing trade commitments and ensure that new trade agreements address IT barriers.**
- **Expand the WTO's Information Technology Agreement.**
- **Intensify bilateral engagement to promote best practices that spur innovation.**

Confronting a New Generation of Market-Access Barriers

As emerging markets become increasingly prosperous, their demand for IT products and services is expanding rapidly. New personal computer sales in China already outstrip sales in the United States, for example,[1] and Brazil recently became the third-largest market for PCs, overtaking Japan.[2] In fact, the four so-called BRIC countries (Brazil, Russia, India, and China) now account for a quarter of all new PC sales globally, up from less than one-sixth in 2006.[3]

This trend shows no signs of diminishing — and it should be good news for the innovative IT industry and the millions of high-wage jobs it supports, since the industry has long looked for global growth opportunities. But the unsettling reality is technology companies are increasingly faced with a new generation of trade barriers in emerging economies. While some tariff barriers remain, most take the form of in-country, "behind-the-border" regulations and requirements. They often are couched as policies to promote innovation, enhance security, or advance other domestic priorities, so they might not on the surface appear to be targeted at foreign suppliers or trade. As such, they can be far more difficult to challenge using traditional WTO rules or trade remedies.

The driving forces behind these market-access barriers are varied:

- Policymakers in emerging markets are seeking to transition their economies away from traditional manufacturing and agriculture to higher-value, innovation-based industries but are following the mistaken belief that insulating domestic suppliers from foreign competition is a viable means to achieve this.
- Governments in many emerging markets recognize that these "behind-the-border" barriers can be more difficult to challenge under existing trade rules and disciplines.
- State-controlled entities play a significant role in the economies of many emerging markets, and governments seek to protect them or use them to achieve political and policy goals.
- Governments in these markets are emulating the practices of China and other key competitors in order to support and defend their own industries, creating a contagion effect that amplifies the global scope of the problem and heightens the urgency of addressing these barriers before they further proliferate.

> "These barriers often are couched as policies to promote innovation, enhance security, or advance other domestic priorities, so they might not on the surface appear to be targeted at foreign suppliers or trade."

The impact of these barriers on the global IT industry is serious and growing. They exclude multinational suppliers or impose costs on them that competing domestic suppliers do not have to bear. This effectively makes products from multinational firms uncompetitive.

1 BARRIER ONE: Restrictions on Procurement by Government Agencies and State-Owned or State-Influenced Enterprises

Given the size and importance of procurement by government agencies and state-owned or state-influenced entities, securing fair and open access to these markets in emerging economies is a high priority for IT suppliers. Measures that exclude multinational suppliers from access to government procurement and procurement by a broad array of state-controlled or state-influenced enterprises translate into high levels of lost exports and jobs. They also deprive governments and other purchasers in emerging markets the ability to choose the best available IT products and services at the best prices.[1]

In many countries, governments are the single largest purchasers of IT products. Combined public sector spending on information and communications technologies worldwide in 2010 was estimated at $423 billion.[2] In emerging economies in particular, governments tend to be disproportionately large purchasers of IT because of the government's deeper involvement in the economy and because governments in these markets are often relatively more intensive IT users.

Notably, no major emerging markets are members of the WTO Government Procurement Agreement (GPA), the core international agreement imposing trade rules on government procurement practices. A few, including China, India, and Turkey, have indicated intent to join the GPA and have begun negotiations or are designated "observers" to the agreement. China pledged to negotiate accession to the GPA "as soon as possible" when it joined the WTO in 2001, yet the negotiations continue.[3]



CASE STUDY

Mandates for Procurement of Domestic Electronic Goods in India

In February 2012, the Indian government issued a notification implementing procurement mandates for domestically manufactured electronic goods. Under this policy, at least 30 percent of procurements are set aside for domestically manufactured products, which are defined as products with a specified percentage of domestic value-add (starting at 25 percent in the first year and increasing to 45 percent after five years). These preferences apply to procurement by government agencies and to procurement by government-licensed entities such as telecommunications service providers and financial services firms. While the full scope of this policy is still unclear, particularly the extent to which it applies to private entities, it represents a highly restrictive policy that could be expanded to a broader range of IT products and services.

The procurement policy for domestically manufactured electronic goods follows the release by the Ministry of ICT in October 2011 of three draft interrelated national policy initiatives — the National IT Policy, National Telecom Policy, and National Electronics Policy — to promote the development of ICT industries in India. While these policies seek the laudable goal of enhancing India's ICT sectors, they set a framework for enacting measures to exclude foreign suppliers or impose burdensome requirements on them.



CASE STUDY

Price Preferences for Procurement of Local Goods in Brazil

In late 2010, the Brazilian government enacted a law that imposed sweeping new government procurement preferences for local products.

Law 12.349/2010 gives preference in public tenders to bidders that offer goods and services that are produced in Brazil and are fully compliant with Brazilian technical standards and regulations. The extent of the preference depends on the industry and has yet to be specified by regulation for many IT products, but the law allows a preference margin of up to 25 percent of the price of foreign-origin products and services. The preference may be adjusted depending on studies that establish criteria for how best to generate jobs and innovation in Brazil. In addition, the law allows for procurement of "strategic" ICT goods and services to be restricted to those with indigenously developed technology.

There is broad international consensus that governments benefit by keeping their procurement markets as open as possible. For instance, under the umbrella of APEC negotiations, leaders of Asia-Pacific economies recently agreed to "[p]romote government procurement policies that are transparent, nondiscriminatory, openly pro-competitive, and performance-based, consistent with the APEC Non-Binding Principles on Government Procurement."[1] Similar commitments to open procurement exist in US law, the laws of the European Union (EU) and its member states, and many other countries.

Increasingly, however, governments in emerging economies are manipulating their procurement rules to exclude foreign products and suppliers. In China, for instance, the government has introduced a broad array of "indigenous innovation" policies at various levels of government (central, provincial, and municipal). One path the Chinese government has pursued is to develop catalogs of products to receive preferential treatment, which excludes products that contain IP developed or owned by a foreign entity. Although Chinese leaders have committed in recent bilateral negotiations with the United States to "delink" government procurement from these "innovation" policies,[2] multinational IT suppliers continue to confront this form of discrimination by government agencies at all levels.

Likewise, India and Brazil have recently taken steps to extend extensive procurement preferences to domestic products and suppliers. Indonesia grants procurement preferences designed to maximize the use of local content and encourage domestic sourcing of supplies.

In addition, some emerging markets have pursued measures to mandate or provide significant preferences for procurement of particular technologies. For example, the Brazilian government has pursued numerous efforts over the past decade to enact preferences at the federal, state, and local government levels for the procurement of open-source software over commercial products.[3] Most recently, in December 2011, two Brazilian legislative committees approved draft Law PL 2269/1999, which would require all Brazilian federal government agencies and state-backed companies to favor open-source software in their procurement policies. This legislation is pending further action in the Brazilian Congress. In India, the Department of Higher Education recently circulated a draft information and communications technology (ICT) policy that includes a strong preference for the open-source software licensing model.



CASE STUDY

Central and State-Level Procurement Preferences in Indonesia

Indonesia has issued a series of policies aimed at maximizing procurement of local products for both central- and state-level government entities. Presidential Regulation 54/2010 calls for procuring entities to maximize local content in procurement, use foreign components only when necessary, and designate foreign contractors as subcontractors to local companies. Presidential Regulation 2/2009 calls on state administrations to optimize the use of domestic goods and services and give price preferences for domestic goods and providers. Ministry of Industry Decree (15/2011) establishes an Accelerated Use of Local Product National Team to optimize procurement of local goods and services.

Software today often contains a mix of open-source and proprietary elements. Efforts by governments to prescribe one model over another for procurement undermine competition in the marketplace and restrict the ability of government purchasers to procure the best products to meet their needs.

In the United States, the White House recently reaffirmed its policy of technology neutrality in IT procurement.[7] Similarly, the EU's public procurement law contains an obligation that procurement be nondiscriminatory.[8] Multilateral organizations have taken similar approaches. Under the APEC Technology Principles, member countries have agreed to "promote technology neutral policies and regulations … that will allow flexibility in the choice of technologies in order to ensure competition, maximize benefits for governments, businesses, and consumers, and bridge the development gap."[9]

> A troubling development is the expansion of government procurement restrictions beyond purchases made by government agencies."

A related and troubling development is the expansion of government procurement restrictions beyond purchases made by government agencies. Many of China's procurement preferences appear to cover procurement by state-owned enterprises, a massive sector in China. This is inconsistent with China's efforts to join the GPA and with its existing WTO commitment that the government "would not influence, directly or indirectly, commercial decisions on the part of state-owned or state-invested enterprises, including the quantity, value or country of origin of any goods purchased or sold…"[10] A new directive in India providing preferences for the procurement of domestically manufactured electronic goods would apply beyond government agencies to procurement by state-licensed entities such as telecommunications service providers.

2 BARRIER TWO: Manipulation of Technology Standards

Technology standards play a vital role in facilitating global trade in IT products and services. Internationally recognized and adopted technical standards that are established with industry participation and accepted across markets generate efficiencies and speed the development and distribution of new products and services, allowing consumers to get them faster and at lower cost. Government intrusion into and manipulation of standards-setting processes hampers innovation and creates artificial barriers to trade.

IT companies invest substantial resources to develop and support technology standards that can be used globally and to make them available for licensing on fair, reasonable, and nondiscriminatory (FRAND) terms to companies large and small, regardless of nationality. This process has generated enormous benefits for consumers. Not only has it spurred technology innovation, but experience has shown that standards are most successful when developed in market-led, voluntary, and consensus-based processes. Discriminatory government-mandated standards, by contrast, tend to "freeze" innovation and force consumers and businesses into using products that might not suit their needs.

It is widely recognized that the market should lead in developing and adopting technology standards. For instance, APEC leaders recently agreed to



CASE STUDY

Restrictive Standards Policies and Practices in China

In 2005, China articulated a National Standards Policy to modernize its standards regime. As a result of this policy and further regulations issued in January 2010 (the Disposal Rules for Inclusion of Patents in National Standards), China's Standardization Administration gained authority over a number of Chinese standards development organizations (SDOs). Although the regulations state that, in principle, foreign firms are allowed to participate fully in such committees, there have been reports of SDOs excluding foreign firms from meetings or preventing them from participating in meaningful ways, which in some cases has led to the "capture" of Chinese standards by Chinese domestic firms. Moreover, in order to participate in standard-setting, foreign firms may be required to disclose confidential and proprietary information, including patented technologies, without assurances that such information will be protected.

For example, the Ministry of Industry and Information Technology is developing standards for software asset management, which already has an International Organization for Standardization (ISO) standard. Foreign companies, which have a wealth of information on global software asset management practices, cannot fully participate in this standard development process.

In addition, China's Standardization Administration does not recognize standards developed by highly reputable, industry-led SDOs such as the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C). Instead, it recognizes standards only if they are developed by China's standard-setting committees or a select few others.



CASE STUDY

Unreasonable Terms for Standards-Essential Patents and Preferences for Indigenous Technology in India

In November 2010, the Indian government announced a policy on open standards for e-governance. The goal of the policy is for standards-essential patents to be made available on a royalty-free basis rather than on fair, reasonable, and nondiscriminatory terms (FRAND). This denies patent holders suitable compensation for their intellectual property and dissuades them from participating in standard-setting processes.

Separately, India's Draft National Telecom Policy takes steps to promote new Indian standards for use in the telecommunications industry. It calls for the establishment of a new Telecommunications Standard Development Organization to aid the development of new Indian standards and promote the use of Indian standards internationally. The Draft Telecom Policy encourages the use of local standards to protect national security and specifically promotes Indian-origin SIM cards that are designed to incorporate Indian standards.

"[e]ncourage the use and participation in the development of voluntary, market-led, and global standards that promote innovation, competition, and create global markets for products and services."[56] Similarly, a recent United Nations report on e-government endorsed the principles of standards choice and technology neutrality and warned of the dangers of government mandates: "Mandating a particular technology [standard] will not only prevent government from using the latest and the best but also consign it to using older and perhaps outmoded standards."[57] Most leading economies have adopted policies that are consistent with these principles.

Despite this consensus, some governments have manipulated standard-setting processes in an effort to bolster domestic firms and insulate them from foreign competition.

In China, for instance, regulators have pressed domestic standards development organizations (SDOs) to adopt standards put forward by domestic firms or that implement patented technologies owned by these firms over more widely adopted international standards. As part of its "indigenous innovation" efforts, China has adopted or sought to develop unique Chinese standards in areas including Internet protocols, 3G telecommunications services, wireless local area networks, digital audio and video, radio frequency identification technology, and encryption.

Chinese SDOs also may restrict meaningful foreign participation, which can make it difficult for non-Chinese entities to influence standards development or protect their patents. Separately, China's rules for testing and certifying compliance with standards are often discriminatory and unduly burdensome and provide inadequate protections for confidential commercial information (including software source code) and intellectual property rights. Likewise, India has adopted policies that favor domestic standards and technologies and discourage compensating patent holders for technologies that are essential to standards.

3 BARRIER THREE: Overreaching Security-Related Regulations

Under the guise of protecting national security, implementing stronger cyber-security measures, or otherwise improving "security," emerging-market governments are imposing measures that often stray far into the commercial sphere. These include procurement restrictions or unreasonable testing and certification requirements. These measures and others create barriers for foreign IT products and deny local consumers and businesses access to the best security solutions to meet their needs. In some instances, these measures actually undermine security.

For example, China's Multi-Level Protection Scheme (MLPS) mandates that only Chinese-owned information security and other IT products with core IP that is Chinese-owned can be used in a broad array of information systems. The Indian government imposes costly and burdensome in-country testing and certification requirements on products procured by telecommunications service providers. Russia has licensing requirements for imports of products with encryption technology that has the effect of delaying and impeding imports.

> "Under the guise of improving 'security,' emerging-market governments are imposing measures that often stray far into the commercial sphere."



CASE STUDY

Restrictions on the Procurement of Foreign IT Security Products in China

IT suppliers face a significant security-related market barrier in China's Multi-Level Protection Scheme (MLPS), which classifies information networks in China based on their relative importance to national security, social order, and economic interests. Any information system classified as level three or higher on a scale of one to five is subject to certain restrictions that have the effect of excluding foreign technologies and firms.

For example, only companies owned by Chinese citizens are allowed to supply IT security products for these systems, and the core technology and key components of the products must contain domestic IP.

Because of the broad and nonspecific language used to describe the different classification levels, most of China's large state-owned enterprises and government agencies in the areas of finance, transportation, telecommunications, health, education, and other areas not directly related to security are classified at level three or higher. China's Ministry of Public Security began sending out inspectors in summer 2010 to identify violators. The inspection campaign aims to achieve "full compliance" among systems classified at level three or above by 2012. To satisfy the MLPS requirements, many state-owned enterprises that once procured foreign IT security products have switched to domestic products.

CASE STUDY



Burdensome Security Testing for IT Products in India

In December 2009, India's Department of Telecommunications issued a series of new requirements for telecommunications service providers (TSPs) that would have required hardware and software vendors to transfer technology and escrow source code and other sensitive design elements with the TSPs. These requirements, which were announced as a means of improving the security of India's commercial telecom networks, applied only to imported products. The policy eventually was amended, but it still imposes burdensome requirements.

Beginning April 1, 2013, all network "elements" must be tested and certified by authorized laboratories in India. That will preclude companies from utilizing long-established, internationally accredited laboratories in other countries. The in-country testing and certification is required even though there is no evidence that where the test is performed has any bearing on its accuracy as long as the laboratory has achieved appropriate accreditation.

The new requirements also have a mandatory facility inspection provision: The TSP must ensure that it, the Department of Telecommunications, or other designated agencies are allowed to inspect vendors' "hardware, software, design, development, manufacturing facility, and supply chain" and "subject all software to a security/threat check" at any time while the vendor is supplying equipment to the TSP. These new inspection requirements will impose a barrier on foreign IT companies' ability to sell to Indian telecommunications operators because most of the foreign suppliers' facilities are located outside India, making compliance more costly and cumbersome than for their in-country competitors.

4 BARRIER FOUR: Regulatory Obstacles to Cloud Computing

Cloud computing offers many potential economic benefits. Via the cloud, small- and mid-sized organizations can access powerful computing resources once available only to the largest companies without having to make significant upfront investments in IT installation, maintenance, and support. Because many cloud service models charge on a "pay-as-you-go" basis, the cloud also enables organizations to scale usage up and down as needed. In these and other ways, the cloud can help reduce IT costs and be a powerful productivity enhancer for enterprises in all countries. But to fully seize the economic opportunity that cloud computing offers, it is critical to remove regulatory obstacles sprouting up in many key markets.

A recent study found that IT innovations enabled by the cloud could generate increased business revenue of $1.1 trillion a year by 2015 and that spending on public and private IT cloud services would generate nearly 14 million jobs worldwide from 2011 to 2015.[10] Notably, more than 50 percent of the new jobs created would be for small- and medium-sized businesses. Job growth linked to cloud computing will be spread globally, with nearly 1.2 million jobs created in the United States and Canada and 6.75 million jobs in China and India by the end of 2015.



CASE STUDY

Licensing Requirements Restricting Foreign Companies' Ability to Offer Cloud Services in China

In China, entities wishing to provide value-added telecommunication services ("VATS") are required to have a VATS license. A particular type of VATS license, known as an ICP license, is required to provide commercial Internet content services, including any Web- or cloud-based content services.

VATS licenses are subject to strict regulation and approval by the Ministry of Industry and Information Technology (MIIT) and several other government authorities. With the exception of a specific type of joint venture known as a foreign invested telecommunications enterprise (FITE), foreign invested companies are not eligible to apply for a VATS license (including an ICP license). Because of the strict regulatory requirements for FITEs — for example, foreign investment in the FITE must not exceed 50 percent of the enterprise's equity interest, the registered capital must be at least RMB 10 million ($1.6 million) if the FITE will engage in nationwide or interprovincial services, and the foreign investor must prove that it has successful experience in providing value-added telecommunication services in the relevant field — it is difficult to obtain approval from MIIT to establish a FITE. Moreover, MIIT has specified that the places and facilities necessary to operate the services must be "installed within the coverage scope as prescribed by the Business License," which is generally understood to mean that any servers and data centers used to support cloud services must be located in China. MIIT has reportedly not issued a single ICP license to a foreign enterprise in the past two to three years.

The VATS/ICP requirements have forced foreign companies to consider less attractive and often unworkable alternatives. For example, some foreign cloud providers are entering into licensing arrangements under which the foreign company provides Web services in China through a contractual licensing relationship with a local agent that already holds an ICP license. This licensing model has inherent IP risks, because the foreign company may need to transfer sensitive IP to the Chinese company while having little control over the management and operation of the Web services provided by the local company. Furthermore, cross-border technology license arrangements are subject to the requirements of China's Technology Import and Export Regulations. Under these regulations, the foreign company must guarantee that the licensed technology is complete, accurate, effective, and capable of achieving the agreed technical objectives, and the foreign company is obliged to defend and indemnify the Chinese party against any claim that the technology infringes third-party rights. Meanwhile, because the foreign party is prohibited from placing restrictions upon the Chinese party regarding improvements to the technology, the Chinese party is free to develop derivative works based on the licensed technology and claim the derivative works as its own.

Many governments, recognizing the potential economic opportunity, are reviewing their regulatory regimes to ensure they are cloud-ready and are working to eliminate rules that unnecessarily impede cloud services. In the United States, for example, the Federal government's Chief Information Officer released a *Federal Cloud Computing Strategy* in 2011. That effort includes a "Cloud First" approach intended to promote the use of cloud technologies.[11]

Rules restricting the free flow of data undermine the cloud computing model. While clouds can be located on premises or contained within a given jurisdiction, cloud computing often involves the storage and processing of data in multiple locations and even in multiple countries. Indeed, many of cloud computing's primary advantages — such as reliability, resiliency, economies of scale, and 24-hour service support — can require that data be stored in multiple markets. Confining data within a given country inhibits the ability of cloud service providers to offer these benefits.

While efforts are under way in the EU and other markets to ease the flow of data among jurisdictions, some governments have taken a different path.[12] For example, China, Indonesia, Vietnam, Brazil, Argentina, Chile, Colombia, Peru, and Costa Rica all have adopted or proposed rules that prohibit or significantly restrict companies from transferring personal information out of the domestic territory. In parallel, many markets are beginning to require that data centers be located inside their geographic borders.

Policies that unnecessarily restrict the free flow of data prevent domestic and foreign cloud service providers alike from hosting data in third countries. But such policies often have a disproportionate impact on foreign cloud providers, whose primary data centers are more likely to be located outside of a given country. At a minimum, foreign providers may mirror data on servers in other jurisdictions as backup in case a domestic datacenter or national network fails.



CASE STUDY

Restrictions on Cross-Border Data Flows & Location Requirements for Data Centers in Indonesia and Vietnam

Laws and regulations under consideration in Indonesia and Vietnam are illustrative of efforts under way in many global markets to require in-country data centers and place other restrictions on cross-border data flows.

In Indonesia, the Law on Information and Electronic Transactions (ITE Law, 11/2008) provides regulation of a general nature concerning electronic transactions. It does not specifically relate to, or facilitate, the provision of cloud computing services. In August 2011, the Indonesian government issued a draft amendment that would require data service providers to establish local representation in Indonesia, including local data centers. It follows that cloud services providers would be required to establish in-country cloud data centers.

In Vietnam, the Ministry of Information and Communication is preparing a decree expected to be submitted soon to the prime minister that would impose a number of new licensing and registration requirements on IT services. Under the current draft decree, providers of data center and cloud computing services would face significant restrictions on the cross-border supply of services and would be required to locate entire equipment systems used for providing such services in the country.

In some markets, licensing rules have created significant obstacles to the entry of foreign cloud providers. For example, because appropriate licenses are available to foreign firms only in certain narrow circumstances, the cloud market in China is largely closed to foreign competition.

Subpar privacy rules also have created an obstacle to market access for cloud providers. Users will migrate to the cloud only if they have confidence that their data will be safe there. Accordingly, national privacy regimes should be predictable and transparent and should avoid unnecessarily burdensome restrictions on cloud service providers such as registration requirements for data controllers and cross-border data transfers. Cloud providers should be encouraged to establish privacy policies that are appropriate for the particular cloud service they provide and the business model they use. Key emerging markets for cloud services, including China, India, Indonesia, Thailand, and Turkey, do not yet have adequate data-protection laws in place.

BSA recently released its Global Cloud Computing Scorecard, a comprehensive assessment of the cloud "readiness" of 24 global markets. The Scorecard analyzes and ranks these markets on the basis of their laws and regulations in seven areas: data privacy, cyber-security, cyber-crime, intellectual property, technology interoperability and legal harmonization, free trade, and IT infrastructure.[9]

A key finding of the Scorecard is that a sharp divide in cloud readiness exists between advanced economies and emerging markets. Japan, the United States, and the EU all have established solid legal and regulatory bases to support the growth of cloud computing. Important emerging economies, such as China, India, and Brazil, have the most work to do to integrate themselves into the global cloud market.

> "Policies that unnecessarily restrict the free flow of data prevent domestic and foreign cloud service providers alike from hosting data in third countries."

The Scorecard proposes a seven-point policy blueprint for governments around the world to expand economic opportunity in the cloud:

1. Protect users' privacy while enabling the free flow of data and commerce.
2. Promote cutting-edge cyber-security practices without requiring the use of specific technologies.
3. Battle cyber-crime with meaningful deterrence and clear causes of action against criminals.
4. Provide robust protection and vigorous enforcement against misappropriation and infringement of cloud technologies.
5. Encourage openness and interoperability between cloud providers and solutions.
6. Promote free trade by lowering barriers and eliminating preferences for particular products or companies.
7. Provide incentives for the private sector to invest in broadband infrastructure, and promote universal access to it among citizens.

It is critical for the growth of cloud computing that the elements of this blueprint be aggressively championed in multilateral forums and through engagement with major emerging markets.

5 BARRIER FIVE: Persistent Tariffs

The multilateral Information Technology Agreement (ITA), launched in 1996 under the auspices of the WTO, has had an enormous impact on removing tariff barriers to global trade in IT products. The signatory countries to the ITA agreed to lower tariff barriers on a wide array of IT products. According to a recent report, implementation of the ITA was a key driver in the expansion of global trade in information and communications technology products from $1.2 trillion in 1996 to $4 trillion in 2008.[xiii]

The ITA, however, has not kept pace with IT product development. In the years since the ITA was inaugurated, global IT companies have come out with a broad array of products that are not covered under the agreement, including new types of semiconductor chips, IT-enabled medical devices, and such computer accessories as monitors and speakers, DVD players, and video game consoles. By not keeping pace with technological developments, the ITA does not cover many products that are vital to the business plans of IT companies today. By some estimates, an expanded ITA could remove tariffs on $800 billion or more of global information and communications technology trade.[xiv]

Moreover, while today there are 73 signatory countries to the ITA, several important economies are not members, including Brazil, Chile, and Russia (which is not yet part of the WTO, but is expected to join soon). The lack of participation in the ITA by these critical emerging markets for IT products is

> "The Information Technology Agreement (ITA) has not kept pace with IT product development."

significantly hampering the ability of global companies to sell IT products there and closing off consumers in these countries to products that can enhance their productivity and well-being.

Notably, at the 2011 APEC Leaders' Meeting, the Leaders' Declaration included a call for APEC to "[p]lay a leadership role in launching negotiations to expand the product coverage and membership of the WTO Information Technology Agreement, in order to build on the contribution this Agreement has made to promoting trade and investment and driving innovation in APEC economies."[xv] It is welcome news that the WTO recently announced several parties to the ITA, including the United States, would be starting informal consultations to expand the agreement.

BSA Policy Recommendations

IT companies face significant and growing market-access challenges in selling their products in the world's fastest-growing emerging markets. These include weak protection of intellectual property, restrictions on investment and establishing local operations, and an increasing array of policies that discriminate in particular against foreign IT products.

Leading IT economies should make these IT-focused barriers centerpiece agenda items in bilateral, multilateral, and regional trade discussions. That should include updating WTO frameworks to address these issues and pursuing them in trade agreements such as the Trans-Pacific Partnership (TPP) and regional forums such as APEC. In addition, the US and other governments should employ current trade tools where appropriate and assess whether additional tools are needed to effectively address these challenges.

BSA offers the following action plan:

- **Press trading partners to adopt transparent, nondiscriminatory government procurement policies.** As major purchasers of IT goods and services, governments have a significant impact on the marketplace. It is therefore critical that they select products based on their relative merits, not the ownership of their underlying intellectual property, the origins or nationalities of their suppliers, or the particular technologies they use. Procurement on these terms would benefit both multinational IT companies seeking access to these markets and governments in these markets that would be able to procure the best products to meet their needs. The WTO's Government Procurement Agreement imposes important requirements on parties to open their government procurement but does not cover China, Brazil, India, Indonesia, and other countries with the most significant and growing procurement markets. Renewed efforts should be made to have these countries join the GPA and to do so on terms consistent with other members. Strong provisions on government procurement also should be addressed in regional forums such as APEC and incorporated into new trade agreements such as the TPP.

- **Ensure that commercial procurement by state-owned or state-influenced enterprises is undertaken without government intrusion.** Too often, governments in emerging markets use their control or influence over enterprises that are commercial actors to direct their purchasing decisions in favor of domestic products. Besides shutting out foreign IT products from this large segment of the commercial marketplace, this practice denies purchasing enterprises the opportunity to choose products that can maximize their productivity. Efforts should be pursued in all relevant forums, including the WTO, bilateral, and multilateral trade agreements and in APEC and other regional forums, to clarify and ensure that commercial procurements by state-owned and state-influenced entities are undertaken without government intrusion.
- **Use trade agreements to establish rules that promote market-led technology standards.** The market-led, consensus-based process for the development and use of technical standards followed in the United States and other leading economies is a success. It fosters innovation and trade, and it gives consumers access to better products at lower cost. There should be clear disciplines in trade agreements that require transparency and adequate opportunity for stakeholder participation in the standards development process. Governments should insist on trade provisions that prevent trading partners from manipulating standards to block foreign competition or protect domestic industry sectors.
- **Establish clear rules allowing data to flow across international borders.** The cloud transcends national borders. The IT industry — and cloud computing in particular — will reach its full potential only if companies can invest freely abroad and can easily transfer data among jurisdictions. Governments around the world should press for global trade rules to prevent barriers to the provision of cloud services, such as unnecessary restrictions on cross-border data flows.
- **Advocate for strengthened intellectual property protection and enforcement, and oppose market-access restrictions based on the location of IP ownership or development.** Innovation leadership is built on a foundation of robust IP protection. High rates of software and hardware piracy and counterfeiting are all too common in most major emerging economies, but now we are seeing measures that make local development or ownership of IP rights a condition of eligibility for access to government procurement or other parts of the market. In addition to strongly advocating for improved laws to protect and enforce IP in emerging markets, governments should oppose policies that make local development or ownership of IP a condition for market access, in law or in practice. This will promote job growth and trade on all sides.

- **Enforce existing trade commitments and ensure that new trade agreements address IT barriers.** Some of the new market-access barriers, while novel, do not require new tools to combat; the WTO and other agreements provide remedies. Governments should not hesitate to use these and any other tools at their disposal to challenge IT protectionism. Additionally, governments should seize all available bilateral and multilateral opportunities to press for new trade disciplines that effectively address these next-generation market-access barriers.
- **Advocate for expansion of the Information Technology Agreement.** The ITA has provided enormous benefits to the global economy by reducing tariff barriers in many developed and emerging markets. With the rapid growth of new technologies and IT products, the ITA is in dire need of updating, both to cover a broad range of additional hardware, software, and other IT products and to cover some major emerging markets that are not currently members of the agreement, such as Brazil and Russia (once it formally joins the WTO). Current members of the ITA should lead an effort to expand both the product and country coverage of the agreement.
- **Intensify bilateral engagement with key trading partners to promote best practices that spur innovation.** This should include discussion of the fundamental building blocks for an innovative ecosystem, including appropriate, non-distortive policies to support technology sector growth. For example, the US government has dialogues like this underway with some countries, such as China, providing a model to build on. The IT industry can play an important role in this process.

About BSA

The Business Software Alliance (BSA) is the leading advocate for the global software industry before governments and in the international marketplace. It is an association of world-class companies that invest billions of dollars annually to create software solutions that spark the economy and improve modern life.

BSA serves as the world's premier anti-piracy organization and as a respected leader in shaping public policies that promote technology innovation and drive economic growth.

Through government relations, intellectual property enforcement, and educational activities in markets around the world, BSA protects intellectual property and fosters innovation; works to open markets and ensure fair competition; and builds trust and confidence in information technology for consumers, businesses, and governments alike.

Protecting Intellectual Property & Fostering Innovation

Intellectual property rights (IPR) — copyrights, patents, and trademarks — provide the legal framework for creative enterprise, the bedrock of growing economies. They are also essential to commercial software development, which is the world's largest copyright industry.

By working with policymakers, leading enforcement actions, and conducting public-education initiatives around the world, BSA ensures that respect for IPR pervades the global economy and society.

- **Championing Intellectual Property Rights:** BSA works with governments around the world to ensure intellectual property protections keep pace with new innovations in technology, such as cloud computing.
- **Curbing Software Theft:** BSA conducts vigorous enforcement programs in approximately 50 countries, helping its members guard against software theft by taking legal action against commercial, end-user license infringement, counterfeiting operations, and Internet piracy.
- **Leading Industry Research:** BSA publishes the most authoritative global studies on piracy and its economic impact, illuminating the scope of the problem and helping shape national and international policy responses.
- **Educating the Public:** BSA educates consumers about harms associated with software piracy and offers a groundbreaking training program to help organizations more effectively manage their software assets.

Opening Markets & Ensuring Fair Competition

Open markets are essential to economic growth and prosperity. BSA expands market opportunities for the software industry by working with governments to break down trade barriers and eliminate discriminatory procurement preferences that stifle innovation by skewing competition.

- **Breaking Down Barriers to Growth:** BSA provides policymakers with information, expert analysis and industry insights to promote an open-market agenda. These efforts include a special focus on the so-called 'BRIC' economies of Brazil, Russia, India and China, which are the world's fastest-growing technology markets but also home to rampant piracy.
- **Promoting Technology Neutrality:** BSA encourages fair competition among technologies by promoting internationally recognized standards and unbiased IT-procurement policies for governments.
- **Supporting New Innovations:** BSA works with policymakers around the world to create conditions for new technologies such as cloud computing to flourish. In addition to collaborating on technology standards, this work involves elevating intellectual property protections, harmonizing international legal principles, and addressing other challenges that are beyond the capability or jurisdiction of any one company or government.

Building Trust & Confidence in Technology

Security and privacy undergird trust and confidence in information technology for consumers, businesses and governments. BSA promotes responsible data stewardship and facilitates acceptance and adoption of each new wave of innovation that transforms the technology marketplace and creates value for society.

- **Driving Public-Private Collaboration:** Drawing on the expertise of its members and productive working relationships with public officials, BSA serves as a knowledge center and catalyst to encourage cooperation and forge consensus among industry and governments.
- **Protecting Consumers:** As new technologies emerge, such as cloud computing, BSA and its members develop appropriate privacy and security standards and share their insights with policymakers and regulators.
- **Mapping Policy Solutions:** BSA has developed a global cybersecurity framework to guide governments in crafting policies that effectively deter and punish cybercrime, mitigate threats, inform and protect consumers, and respond to cyber incidents.

Endnotes

[1] Michael Kan, China Overtakes US in PC Sales Earlier Than Expected, PC World (Aug. 23, 2011).

[2] Rajani Singh & David Daoud, IDC, Worldwide PC Market: 1Q11 Review (July 2011).

[3] Business Software Alliance, Emerging Markets at a Glance.

[4] The US Buy American Act (41 U.S.C. sec 10a-10d) provides a much more limited range of restrictions on procurement of foreign products than the measures arising in many emerging markets. In addition, by law, the US Congress has since 2004 annually waived application of the Buy America Act to procurement of commercial-item IT products.

[5] Publictechnology.net & Gartner, Global ICT Public Sector Spend Outstrips Market (Aug. 19, 2010).

[6] WTO, Working Party on the Accession of China — Report of the Working Party on the Accession of China, 340–341 (Oct. 1, 2011).

[7] APEC, 2011 Leaders' Declaration, Annex A: Promoting Effective, Non-Discriminatory, and Market-Driven Innovation Policy (Nov. 13, 2011).

[8] United States Trade Representative Office, 2011 U.S.-China Joint Commission on Commerce and Trade Outcomes (Nov. 2011); see also US Department of the Treasury, The 2011 U.S.-China Strategic and Economic Dialogue U.S. Fact Sheet — Economic Track (May 10, 2011).

[9] Open-source software is a licensing model where the source code of the software is typically made available royalty-free to the users of the software, under terms allowing redistribution and modification with certain restrictions. "Commercial software" refers to software developed by a commercial entity that is typically licensed for a fee to a customer subject to certain conditions.

[10] Executive Office of the President, Office of Management and Budget, Memorandum for Chief Information Officers and Senior Procurement Executives (Jan. 7, 2011).

[11] Article 23, Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts, and public service contracts.

[12] Asia-Pacific Economic Cooperation, APEC Principles for Technology Choice Pathfinder (Sept. 1, 2006).

[13] WTO, Working Party on the Accession of China — Report of the Working Party on the Accession of China, 46 (Oct. 1, 2011).

[14] APEC, 2011 Leaders' Declaration, Annex A: Promoting Effective, Non-Discriminatory, and Market-Driven Innovation Policy (Nov. 13, 2011).

[15] United Nations Development Programme, e-Government Interoperability: Guide, at 10 (2007).

[16] IDC, Cloud Computing's Role in Job Creation (March 2012).

[17] Vivek Kundra, White House, Federal Cloud Computing Strategy (Feb. 8, 2011).

[18] Even in the EU, where efforts are under way to ease the flow of data among member states, some countries are taking steps that would undermine that effort. In Germany, for example, restrictive interpretations of existing laws and policies are being used to justify requirements for geographic restrictions on data. Such restrictions in developed economies are especially damaging in that they can be used by emerging markets to legitimize their own market-access barriers.

[19] BSA Global Cloud Computing Scorecard (Feb. 22, 2012).

[20] Information Technology and Innovation Foundation, Boosting Exports, Jobs, and Economic Growth by Expanding the ITA, at 1 (March 2012).

[21] Information Technology and Innovation Foundation, Boosting Exports, Jobs, and Economic Growth by Expanding the ITA, at 2 (March 2012).

[22] APEC, 2011 Leaders Declaration (Nov. 12–13, 2012).


BSA
BUSINESS SOFTWARE ALLIANCE
www.bsa.org
BSA Worldwide Headquarters
1150 18th Street, NW
Suite 700
Washington, DC 20036
T: +1.202.872.5500
F: +1.202.872.5501
BSA Asia-Pacific
300 Beach Road
#25-08 The Concourse
Singapore 199555
T: +65.6292.2072
F: +65.6292.6369
BSA Europe, Middle East & Africa
2 Queen Anne's Gate Buildings
Dartmouth Street
London, SW1H 9BP
United Kingdom
T: +44.207.340.6080
F: +44.207.340.6090
Bangkok, Thailand Beijing, China Brussels, Belgium Hanoi, Vietnam Jakarta, Indonesia Kuala Lumpur, Malaysia
München, Germany New Delhi, India São Paulo, Brazil Taipei, Taiwan Tokyo, Japan


BSA GLOBAL CLOUD
COMPUTING SCORECARD
A Blueprint for Economic Opportunity
BSA
Business Software Alliance
galexia
CONSULTING



CONTENTS

EXECUTIVE SUMMARY 1
BSA Cloud Policy Blueprint 2
KEY FINDINGS 3
Measuring Cloud Computing Readiness 4
Data Privacy 4
Security 5
Cybercrime 5
Intellectual Property Rights 6
Support for Industry-Led Standards & International Harmonization of Rules 6
Promoting Free Trade 7
ICT Readiness, Broadband Deployment 7
BSA GLOBAL CLOUD COMPUTING SCORECARD 8
SCORECARD METHODOLOGY 10
USING THE SCORECARD 10
BSA GLOBAL CLOUD COMPUTING COUNTRY CHECKLIST 12
ABOUT BSA 20

EXECUTIVE SUMMARY

In small and large enterprises as well as government offices around the world, one thing has become perfectly clear: Cloud computing marks the next contribution that software and computing technologies will make toward greater productivity and expanded economic growth.

The BSA Global Cloud Computing Scorecard provides a roadmap for the initiatives and policies that countries can — and should — take to ensure that they reap the full economic and growth benefits. It is well established that each of the individual elements of the scorecard is critical to economic growth and job creation. They are especially critical in the context of cloud computing because the cloud provides a positive multiplier opportunity. Executing on these policies will promote innovation; cloud computing will ensure that innovation is fully harnessed and realized.

The BSA Global Cloud Computing Scorecard provides a roadmap for the initiatives and policies that countries can — and should — take to ensure that they reap the full economic and growth benefits.

The Scorecard finds a sharp divide between advanced economies and the developing world when it comes to cloud readiness. Japan, the United States and the European Union member states, for example, have each established a solid legal and regulatory base to support the growth of cloud computing. This is significant because the full benefits of a global cloud computing environment require a broad network of effective laws and regulations. Only in that way will the potential efficiencies and economies of scale enabled by the cloud truly take hold.

The cloud-ready legal and regulatory environments of these countries provide models for those in the bottom half of the Scorecard — including India, China and Brazil. And these models take on additional importance when you factor in the expected growth in the markets that finished toward the bottom of the Scorecard rankings. As millions of new consumers and small businesses around the world gain access to an Internet-enabled environment, the global economy will gain — and grow — most when they have the full power of the cloud at their fingertips. Such access, though, will require significant legal and regulatory reforms.

Cloud computing is not any one thing. It is a mix of software-enabled resources and services that can be delivered to the user on an "as needed" basis. As the National Institute of Standards and Technology puts it: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

What is more important — and more understandable — are the economic and social benefits inherent in cloud computing. For small and large businesses, governments and consumers, it equalizes access to

technology. It allows individuals to enjoy the benefits that large users have long enjoyed, opening the door to vastly greater enhancements in efficiency, productivity and competitiveness for businesses in the global marketplace. For governments, cloud computing presents a two-fold opportunity: the chance to improve productivity and citizen engagement through IT procurements as well as the benefit of encouraging economic growth, sustainable job creation and higher wages and standards of living by encouraging the IT economy.

Cloud computing is a technological paradigm that is certain to be a new engine of the global economy. Attaining those benefits will require governments around the world to establish the proper legal and regulatory framework to support cloud computing.

BSA CLOUD POLICY BLUEPRINT

The economic growth predicted to flow from cloud computing — and the resulting transformation of both businesses and national economies — is predicated on the proper policies being in place in each of the seven areas used in the BSA index:

- Ensuring privacy: The success of cloud computing depends on users' faith that their information will not be used or disclosed in unexpected ways. At the same time, to maximize the benefit of the cloud, providers must be free to move data through the cloud in the most efficient way.
- Promoting security: Users must be assured that cloud computing providers understand and properly manage the risks inherent in storing and running applications in the cloud. Cloud providers must be able to implement cutting-edge cybersecurity solutions without being required to use specific technologies.
- Battling cybercrime: In cyberspace, as in the real world, laws must provide meaningful deterrence and clear causes of action. Legal systems should provide an effective mechanism for law enforcement, and for cloud providers themselves, to combat unauthorized access to data stored in the cloud.
- Protecting intellectual property: In order to promote continued innovation and technological advancement, intellectual property laws should provide for clear protection and vigorous enforcement against misappropriation and infringement of the developments that underlie the cloud.
- Ensuring data portability and the harmonization of international rules: The smooth flow of data around the world — as with between different cloud providers — requires efforts to promote openness and interoperability. Governments should work with industry to develop standards, while also working to minimize conflicting legal obligations on cloud providers.
- Promoting free trade: By their very nature, cloud technologies operate across national boundaries. The cloud's ability to promote economic growth depends on a global market that transcends barriers to free trade, including preferences for particular products or providers.
- Establishing the necessary IT infrastructure: Cloud computing requires robust, ubiquitous and affordable broadband access. This can be achieved through policies that provide incentives for private sector investment in broadband infrastructure and laws that promote universal access to broadband.

The move to the cloud and capitalization on its benefits across the board is hardly inevitable, and an urgent task lies ahead for governments. In order to obtain the benefits of the cloud, policymakers must provide a legal and regulatory framework that will promote innovation, provide incentives to build the infrastructure to support it, and promote confidence that using the cloud will bring the anticipated benefits without sacrificing expectations of privacy, security and safety.

KEY FINDINGS

The first-of-its-kind BSA Global Cloud Computing Scorecard ranks 24 countries accounting for 80 percent of the global ICT market based on seven policy categories that measure the countries' preparedness to support the growth of cloud computing. This unprecedented insight into the laws and regulations of markets around the world provides a window into which countries are best poised to capitalize on the technological and economic benefits of cloud computing.

Among other findings: The Scorecard reveals that while developed nations are more "cloud ready" than developing economies, troubling obstacles emerge when you examine the lack of alignment in the legal and regulatory environments in many of those advanced countries. A healthy national market for cloud computing does not necessarily translate into a market that is "in harmony" with the laws of other countries in a way that will allow for the smooth flow of data across borders. It is this kind of harmony that is needed to advance the growth of cloud computing at the level that will allow it to truly take advantage of its global efficiencies.

All countries, regardless of their level of economic development, could benefit from coordinated policy responses for the government and the public to fully benefit from cloud computing.

As in broader measures, the Scorecard finds two worlds exist when it comes to cloud preparedness: Advanced economies like Japan — the Scorecard's top finisher — have laws and regulations that promise to support the development of cloud computing. Less-developed economies, such as last-place finisher Brazil, face several challenges when it comes to fully capitalizing on the economic benefits of the cloud.

Further, countries on both sides must be vigilant not to take steps that would hurt their chances of growing the cloud market. Already many countries plan new laws that will help them advance in the digital economy. Some — such as Mexico's new privacy law — have the potential to advance a country's score. Others — such as the proposed Data Protection Regulation in the European Union, which has the potential to undermine its benefits with new, overly prescriptive rules — threaten to undermine the economic advances that a truly global cloud can provide.

Those interested in advancing cloud computing can find a model in Japan. The country is a leader in cloud readiness and easily topped the Scorecard rankings. Japan has a comprehensive suite of modern laws that support and facilitate the digital economy and cloud computing — from comprehensive privacy legislation that avoids burdens on data transfers and data controllers to a full range of criminal and IP law protections. Further, Japan is a leader in the

development of international standards related to cloud computing, and the country is working to provide all households with high-speed fiber broadband connections in the next three years.

Perhaps fittingly, the countries with the most room for improvement are those countries where ICT sector growth will be most dramatic in the coming years. Consider China, for example. According to the research firm IDC, the size of China's ICT sector is expected to nearly double between 2010 and 2015, going from $221 billion to $389 billion. International companies, however, confront several obstacles to growth in China, however, including extensive regulation of Internet content and the continued promotion of policies that discriminate against foreign technology companies.

Countries must take care not to adopt new policies that inhibit the development of the global cloud economy. Already, some countries are placing geographic restrictions on data and considering other limits on outsourcing of work or offshoring of data.

The scorecard is a snapshot of the current legal and regulatory regimes in the countries examined. Already, countries around the world are moving to adapt their laws and regulations to help boost cloud computing. Some of these are captured here including, for example, new laws on privacy in India, Korea, and Mexico, while other reforms are expected in the coming months and years.

Finally, countries must take care not to adopt new policies that inhibit the development of the global cloud economy. Already, some countries are placing geographic restrictions on data and considering other limits on outsourcing of work or offshoring of data.

Germany, for example, is a country that scores well in the initial Scorecard, but it threatens to undermine that advantage with overly restrictive legal interpretations to keep some data within national borders.

It is also clear in most categories that numerous issues remain to be addressed and that all countries, regardless of their level of economic development, could benefit from coordinated policy responses for the government and the public to fully benefit from cloud computing.

MEASURING CLOUD COMPUTING READINESS

The Scorecard examines major laws and regulations relevant to cloud computing in seven policy categories as well as each country's ICT-related infrastructure and broadband deployment. These policy categories align with the BSA's Cloud Computing Guiding Principles, which underpin the Scorecard's analytical framework and its suggestions for providing a workable framework to allow for the growth of cloud computing.

Data Privacy

This section of the Scorecard examines data privacy regulation and the presence and structure of privacy regulators in each jurisdiction. The section also examines registration requirements for data controllers and data breach notification requirements.

The Scorecard reveals that most countries have data protection laws in place and have established independent privacy commissioners. Many of these laws are based on a mix of the OECD Guidelines, the EU Directive or the APEC Privacy Principles. Unfortunately, registration requirements for data controllers or data transfers may act as barriers to the take-up of cloud services. Such requirements are common in some countries, including requirements for registering cross-border transfers in some EU countries.

Korea, which replaced its patchwork of privacy protections with modern and comprehensive legislation in 2011, scored 9.3 out of 10 available points to top the Scorecard's rankings in the privacy section. At the other end of the spectrum, South Africa finished with just 2.8 points.

The Scorecard also reveals substantial pending data protection law reform, with major reviews and proposals in China, the European Union, India, Singapore, South Africa and the United States. This is an area of rapid legal development. Unfortunately, some key jurisdictions, including China, India, Indonesia and Singapore do not yet have any substantial data protection laws in place.

Such developments are important because cloud users will fully accept and adopt cloud computing only if they are confident that private information stored in the cloud, wherever in the world, will not be used or disclosed by the cloud provider in unexpected ways. National privacy regimes should be predictable, transparent and avoid unnecessarily burdensome restrictions on cloud service providers such as registration requirements for data controllers and cross-border data transfers. Cloud providers should be encouraged to establish privacy policies that are appropriate for the particular cloud service they provide and the business model they use.

Security

Consumers of cloud computing and other digital services (including both private-sector and government users) need assurance that cloud service providers understand and appropriately manage the security risks associated with storing their data and running their applications on cloud systems. This section of the Scorecard examines whether security criteria and the ongoing testing of security measures are the subject of regulation in each jurisdiction. The Security section also examines electronic signature laws and Internet censorship or filtering requirements. Japan tops the Scorecard's security section with 8.4 of the 10 available points; Thailand's regime, on the other end of the scale, nets just 1.6 points.

The Scorecard reveals that most countries do have clear, technology neutral electronic signature laws. In addition, security requirements are in place in most jurisdictions, and security audit requirements were generally absent.

A number of countries — ranging from advanced markets like Korea (6.0 points on security) to developing countries like India (4.4) — have implemented Internet filtering or censorship regimes that may act as a barrier to the expansion of the digital economy and cloud computing. Some such regimes regulate criminal conduct, including distribution of illegal material, particularly child pornography. However, a number of the filtering or censorship schemes appear to include a strong political element, in that they regularly block sites that expressed political dissent. China, for example, restricts access to online content under a large and complex legal and technical regime that invokes the protection of national security and social order. This factor played a significant factor in China scoring just 2.0 points in the security section.

Cybercrime

As cloud computing involves the aggregation of massive amounts of data in large data centers, it creates new and highly tempting targets. As criminals turn their attention to these vaults of information, it will become increasingly challenging to protect such data centers from both physical and cyber attacks. Governments should ensure that domestic laws provide an effective mechanism for law enforcement, and for cloud providers themselves, to combat unauthorized access to data stored in the cloud. This section examines these issues as well as rules relating to investigation and enforcement, including access to encrypted data and extraterritorial offences.

As cloud computing involves the aggregation of massive amounts of data in large data centers, it creates new and highly tempting targets.

The Scorecard finds that most countries have either computer crime legislation or cybercrime legislation, and many laws are broadly compliant with the Convention on Cybercrime. Many countries in the study (the EU members, Japan and the United States) have signed the Convention, and several other countries are considering

signing (Australia and Mexico are close). Unfortunately, a few key jurisdictions still have gaps and inconsistencies in their cybercrime laws. Canada, for example, signed the Council of Europe Cybercrime Convention in 2001, but it has failed to ratify the Convention for more than a decade. And while the country has a comprehensive computer crime law in place, it lacks essential online investigation and enforcement tools. Thus, while Japan, German and France scored a perfect 10.0 points in the cybercrime section, Canada trailed 6.2 points.

Cloud services operate across national boundaries, and their success depends on access to regional and global markets. Restrictive policies that create actual or potential trade barriers will slow the evolution of cloud computing.

This section also examines rules on investigation and enforcement, including access to encrypted data and extraterritorial offences. There is a greater divergence in results in these fields.

Intellectual Property Rights

Providers of cloud computing and digital economy technologies and services, as with other highly innovative products, rely on a combination of patents, copyrights, trade secrets and other forms of intellectual property protection. Thus, to encourage investments in cloud R&D and infrastructure, IP laws must provide strong incentives for these investments and clear protection and vigorous enforcement against misappropriation and infringement. Online intermediaries should have incentives to behave responsibly, and they should enjoy safe harbors from liability when they do so.

The Scorecard reveals that countries are moving toward a consistent approach on many key rights and protections. Gaps exist, however, in the IP laws of key jurisdictions, including Canada, India and Thailand. Russia, which finished in the 16th in the overall Scorecard rankings and far back in the IP section with just 8.4 out of 20 available points, serves as a prime example. The country was slow to make any progress on its bid to join the Agreement on Trade Related Aspects of Intellectual Property Rights, or TRIPS Agreement over several years. This and other holes in the country's IP regime could expose cloud computing services to risks.

This section also examines investigatory and enforcement approaches, where there is a wide diversity of approaches and significant inconsistency. Concerns also exist about the enforcement culture and resources available in some jurisdictions. Even countries with up-to-date IP laws sometimes fail to enforce these laws, and piracy rates remain high in many jurisdictions.

Support for Industry-Led Standards & International Harmonization of Rules

Data portability and seamless use of interoperable applications are key considerations for cloud computing and digital economy applications. Consumers are demanding interoperability in the cloud computing space, and industry is working hard through standards development organizations and other international avenues to meet this demand. Government support of these efforts is important.

This section of the Scorecard examines whether or not governments encourage standards to be developed through voluntary, industry-led standards processes. This section also examines international harmonization of e-commerce rules, tariffs and relevant trade rules.

The Scorecard reveals that governments take an inconsistent approach to standards development and that many ad hoc decisions are made in the absence of national frameworks and policies. Many countries have well-established frameworks for standard-setting, and the United States' National Institute for Standards and Technology is carefully eyeing cloud computing. The United States finished toward the top of this

section, scoring 9.4 out of 10 points. At the other end of the scale, countries like Argentina (4.6) and Brazil (3.4) lack even a relevant framework for ICT standards. Government agencies should work with industry to accelerate standards development, where appropriate, and share user requirements with open standard setting organizations.

As it relates to e-commerce rules, tariffs and relevant trade rules, the Scorecard finds a great deal of consistency in e-commerce laws, with most countries implementing laws based on the UNCITRAL Model Law on E-Commerce and / or the UN Convention on Electronic Contracting. Several countries, including Singapore, Russia and Malaysia, have signed / ratified the Convention, leading to even greater harmonization. Tariffs and trade barriers for online software and applications are rare, although a few jurisdictions still maintain tariffs on new technology products that are used to access cloud services.

Promoting Free Trade

Cloud services operate across national boundaries, and their success depends on access to regional and global markets. Restrictive policies that create actual or potential trade barriers will slow the evolution of cloud computing.

This section of the Scorecard examines and compares government procurement regimes and efforts to remove barriers to free trade, including countries' requirements and preferences for particular products.

The Scorecard finds that a number of jurisdictions that still provide preferential treatment for domestic suppliers in government procurements, including Brazil (2.2 of 10 points), China (4.8), and Malaysia (3.8). In a positive development, Japan (9.2 points) and a growing number of other countries have become members of the WTO Agreement on Government Procurement, which liberalizes such policies.

ICT Readiness, Broadband Deployment

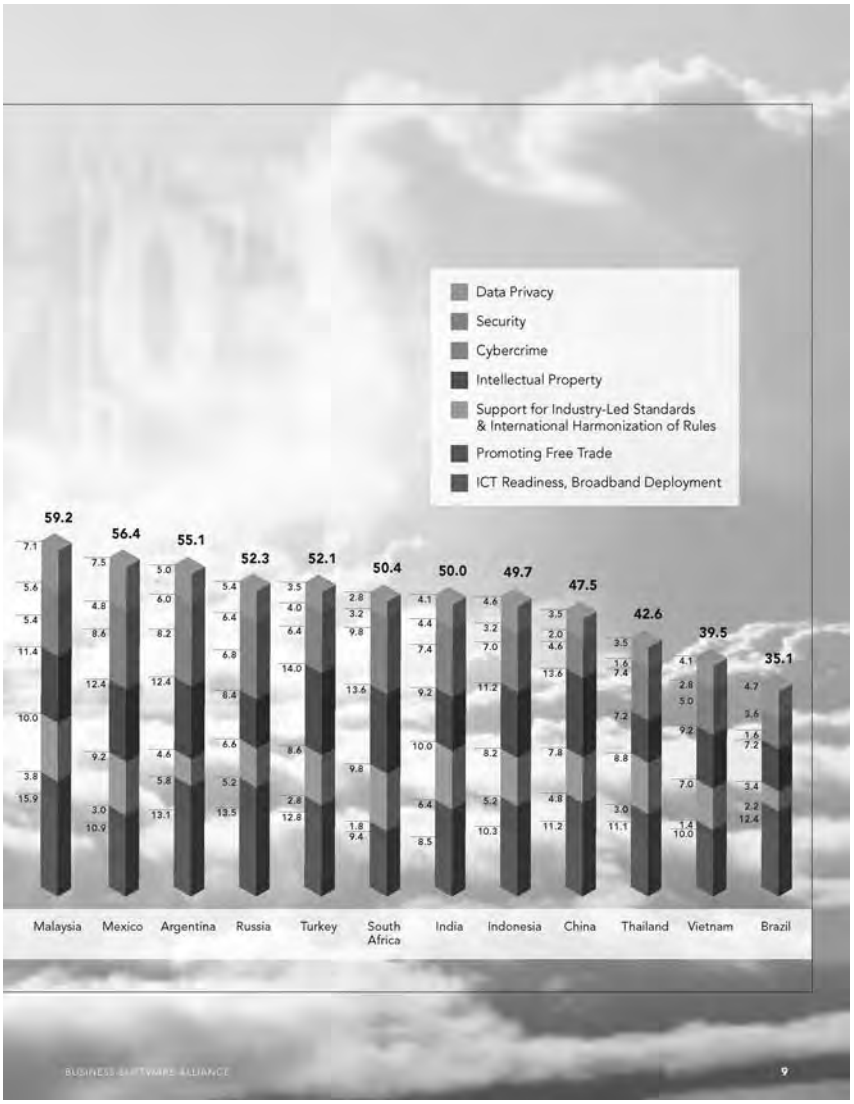
Cloud computing can achieve its full potential only if there is robust, ubiquitous and affordable broadband access. This can be achieved through policies that provide incentives for private sector investment in broadband infrastructure and laws that promote universal access to broadband.

This section of the Scorecard examines and compares the infrastructure that is available in each economy to support the digital economy and cloud computing. This section benefits from the inclusion of statistics on the number of subscribers for various products, reflecting the importance (and growth) of mobile broadband subscriptions.

Cloud computing can achieve its full potential only if there is robust, ubiquitous and affordable broadband access.

Several countries have implemented impressive national broadband networks, including Japan (20.9 out of 30 points), Singapore (21.8) and Korea (21.7). Major infrastructure improvements are under way in Australia (21.3) and a range of EU countries. Broadband penetration remains very inconsistent, however, and there is a risk that some countries do not yet have the infrastructure in place to take full advantage of the digital economy and cloud computing. Progress lags, however, in countries like India (8.5) and South Africa (9.4).


BSA Global Cloud Computing Scorecard
The first-of-its-kind BSA Global Cloud Computing Scorecard ranks 24 countries based on seven policy categories that measure the countries' preparedness to support the growth of cloud computing. Together, these countries account for 80 percent of the global ICT market.
83.3
79.2
79.0
78.6
78.4
76.6
76.6
76.0
73.9
72.2
70.7
70.4
Japan
Australia
Germany
United States
France
Italy
United Kingdom
Korea
Spain
Singapore
Poland
Canada


Data Privacy
Security
Cybercrime
Intellectual Property
Support for Industry-Led Standards & International Harmonization of Rules
Promoting Free Trade
ICT Readiness, Broadband Deployment
59.2
7.1
5.6
5.4
11.4
10.0
3.8
15.9
56.4
7.5
4.8
8.6
12.4
9.2
3.0
10.9
55.1
5.0
6.0
8.2
12.4
4.6
5.8
13.1
52.3
5.4
6.4
6.8
8.4
6.6
5.2
13.5
52.1
3.5
4.0
6.4
14.0
8.6
2.8
12.8
50.4
2.8
3.2
9.8
13.6
9.8
1.8
9.4
50.0
4.1
4.4
7.4
9.2
10.0
6.4
8.5
49.7
4.6
3.2
7.0
11.2
8.2
5.2
10.3
47.5
3.5
2.0
4.6
13.6
7.8
4.8
11.2
42.6
3.5
1.6
7.4
7.2
8.8
3.0
11.1
39.5
4.1
2.8
5.0
9.2
7.0
1.4
10.0
35.1
4.7
3.6
1.6
7.2
5.4
2.2
12.4
Malaysia
Mexico
Argentina
Russia
Turkey
South Africa
India
Indonesia
China
Thailand
Vietnam
Brazil
BUSINESS SOFTWARE ALLIANCE
9

SCORECARD METHODOLOGY

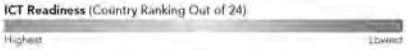
The BSA Global Cloud Computing Scorecard examines the legal and regulatory framework of 24 countries around the world, identifying 66 questions that are relevant to determining readiness for cloud computing. The questions are categorized under the aforementioned policy categories, and are generally framed so as to be answerable by "yes" or "no." The answers are also color coded:

- ✔ Indicates a positive assessment, which is generally considered to be an encouraging step towards the establishment of a favorable legal and regulatory environment for cloud computing.
- ✖ Indicates a negative assessment and the presence of a potential barrier to the establishment of a favorable legal and regulatory.
- ◑ Indicates that the assessment is positive in part, although some gaps or inconsistencies may exist which require further remedial work.
- Indicates a fact-finding question on relevant issues.

The Scorecard aims to provide a platform for discussion between policymakers and providers of cloud offerings, with a view toward developing an internationally harmonized regime of laws and regulations relevant to cloud computing. It is a tool that can help policymakers conduct a constructive self-evaluation, and determine the next steps that need to be taken to help advance the growth of global cloud computing.

Responses for the infrastructure portion of the Scorecard are color coded based on the scale below. That is, the "highest" answer to a particular question (e.g., the largest population or highest number of internet users) is indicated in bright green, and the color for other responses graduates down to the lowest response in red.

ICT Readiness (Country Ranking Out of 24)



Highest Lowest

USING THE SCORECARD

The Scorecard is derived from the Country Reports — a weighted score has been allocated to a selection of key questions. A number of basic fact-finding questions are excluded from the scoring system. Each group of questions is weighted to reflect its importance to cloud computing. Each individual question is also weighted to reflect its importance within each group. The weights are shown in the following table:

#	THEME / QUESTIONS	Weight	Value (out of 100)
DATA PRIVACY		**10%**	**10**
1.	Are there laws or regulations governing the collection, use or other processing of personal information?	30%	3
6.	Is there an effective agency (or regulator) tasked with the enforcement of privacy laws?	25%	2.5
8.	Are data controllers free from registration requirements?	20%	2
9.	Are cross border transfers free from registration requirements?	15%	1.5
10.	Is there a breach notification law?	10%	1
SECURITY		**10%**	**10**
1.	Is there a law or regulation that gives electronic signatures clear legal weight?	20%	2
2.	Are ISPs and content service providers free from mandatory filtering or censoring?	20%	2
3.	Are there laws or enforceable codes containing general security requirements for digital data hosting and cloud service providers?	20%	2
4.	Are there laws or enforceable codes containing specific security audit requirements for digital data hosting and cloud service providers?	20%	2
5.	Are there security laws and regulations requiring specific certifications for technology products?	20%	2

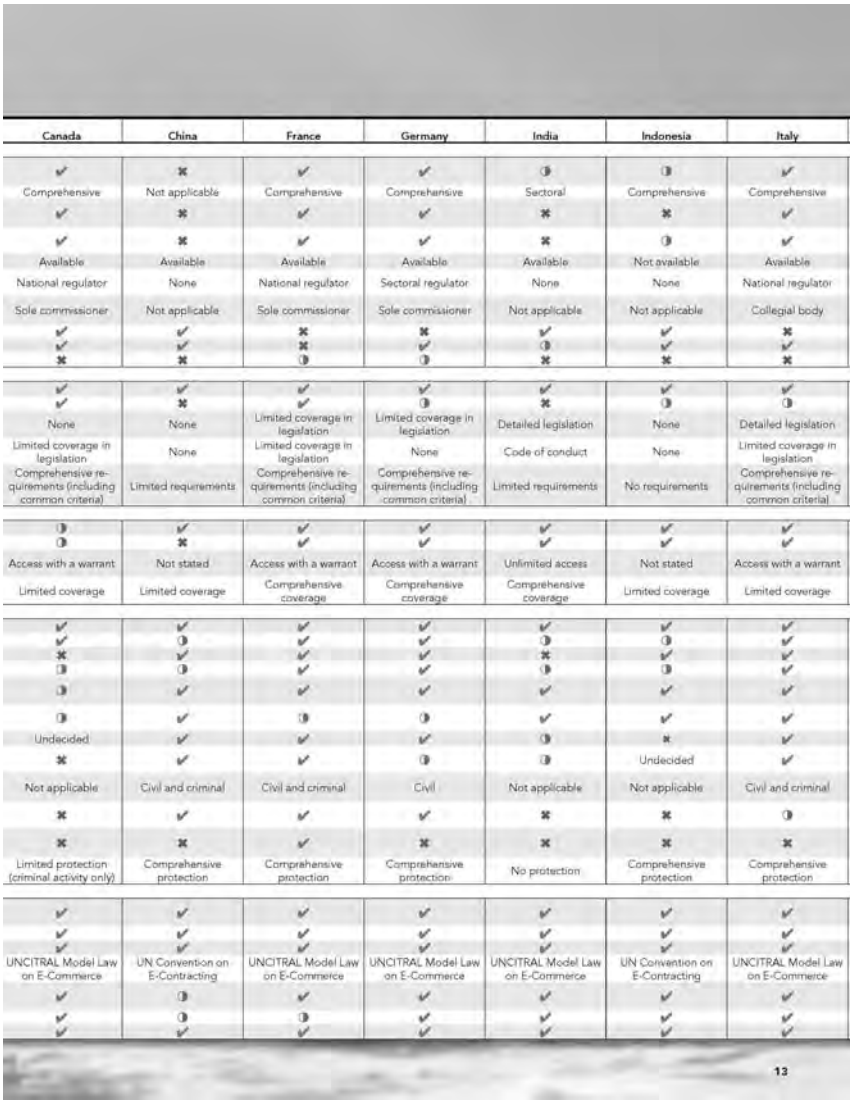
#	THEME / QUESTIONS	Weight	Value (out of 100)
CYBERCRIME		**10%**	**10**
1.	Are there cybercrime laws in place?	50%	5
2.	Are cybercrime laws consistent with the Budapest Convention on Cybercrime?	30%	3
3.	What access do law enforcement authorities have to encrypted data held or transmitted by data hosting providers, carriers or other service providers?	10%	1
4.	How does the law deal with extraterritorial offenses?	10%	1
INTELLECTUAL PROPERTY		**20%**	**20**
1.	Is the country a member of the TRIPS Agreement?	10%	2
2.	Have IP laws been enacted to implement TRIPS?	10%	2
3.	Is the country party to the WIPO Copyright Treaty?	10%	2
4.	Have laws implementing the WIPO Copyright Treaty been enacted?	10%	2
5.	Are civil sanctions available for unauthorized making available (posting) of copyright holders' works on the Internet?	10%	2
6.	Are criminal sanctions available for unauthorized making available (posting) of copyright holders' works on the Internet?	10%	2
7.	Are there laws governing ISP liability for content that infringes copyright?	5%	1
8.	Is there a basis for ISPs to be held liable for content that infringes copyright found on their sites or systems?	5%	1
10.	Must ISPs takedown content that infringes copyright, upon notification by the right holder?	5%	1
11.	Are ISPs required to inform subscribers upon receiving a notification that the subscriber is using the ISP's service to distribute content that infringes copyright?	5%	1
12.	Is there clear legal protection against misappropriation of cloud computing services?, including effective enforcement?	20%	4
SUPPORT FOR INDUSTRY-LED STANDARDS & INTERNATIONAL HARMONIZATION OF RULES		**10%**	**10**
1.	Are there laws, regulations or policies that establish a standards setting framework for interoperability and portability of data?	30%	3
2.	Is there a regulatory body responsible for standards development for the country?	10%	1
3.	Are e-commerce laws in place?	30%	3
4.	Is the downloading of applications or digital data from foreign cloud service providers free from tariff or other trade barriers?	10%	1
5.	Are international standards favored over domestic standards?	10%	1
6.	Does the government participate in international standards setting process?	10%	1
PROMOTING FREE TRADE		**10%**	**10**
1.	Are there any laws or policies in place that implement technology neutrality in government?	20%	2
2.	Are cloud computing services able to operate free from laws or policies that mandate the use of certain products (including, but not limited to types of software), services, standards or technologies?	20%	2
3.	Are cloud computing services able to operate free from laws or policies that establish preferences for certain products (including, but not limited to types of software), services, standards, or technologies?	10%	1
4.	Are cloud computing services able to operate free from laws that discriminate based on the nationality of the vendor, developer or service provider?	50%	5
ICT READINESS, BROADBAND DEPLOYMENT		**30%**	**30**
1.	Is there a National Broadband Plan?	13%	3.75
3.7.	Personal Computers (% of households) (2010)	3%	0.75
4.1.	ITU ICT Development Index (IDI) (2010) (Score is out of 10 and includes 152 countries)	20%	6
4.2.	World Economic Forum Networked Readiness Index (2010–2011) (Score is out of 7 and includes 138 countries)	20%	6
4.3.	International Connectivity Score (2011) (Score is out of 10 and includes 50 countries)	15%	4.5
4.4.	IT Industry Competitiveness Index (2011) (Score is out of 100 and includes 66 countries)	10%	3
5.2.	Internet Users as Percentage of Population (2010)	5%	1.5
5.3.	International Internet Bandwidth (bits per second per internet user) (2010)	3%	0.75
5.4.	International Internet Bandwidth (2010) (total gigabits per second (Gbps) per country)	3%	0.75
6.4.	Fixed Broadband Subscriptions as % of Internet users (2010)	5%	1.5
7.2.	Active mobile-broadband subscriptions per 100 inhabitants (2010)	5%	1.5



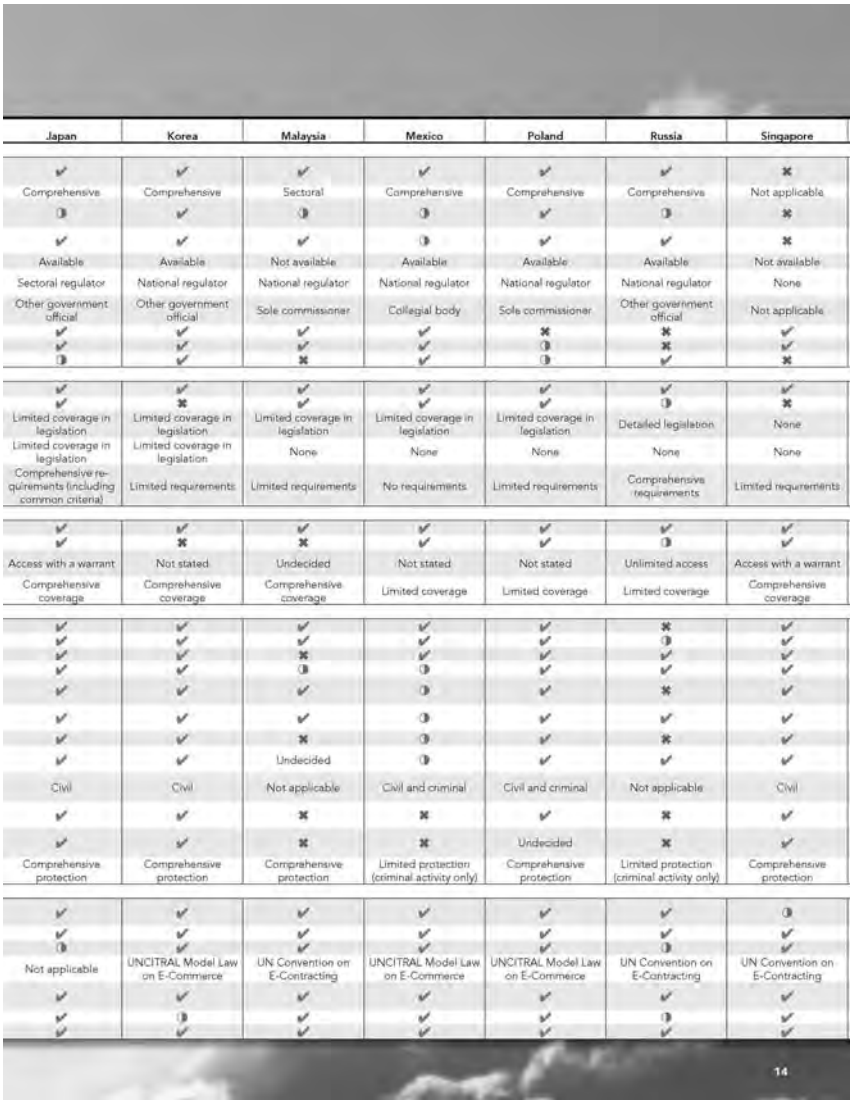
BSA Global Cloud Computing Country Checklist

✔ Yes ✖ No ◑ Partial

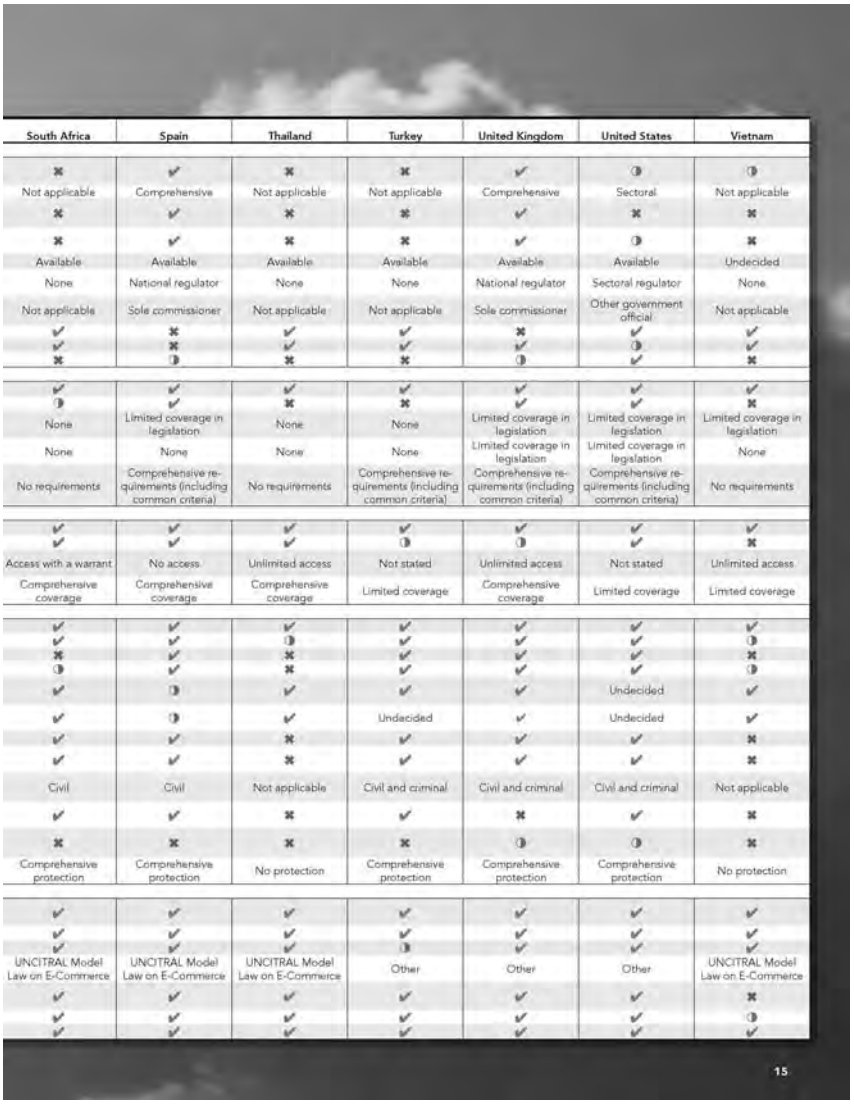
#	QUESTION	Argentina	Australia	Brazil
	DATA PRIVACY			
1.	Are there laws or regulations governing the collection, use or other processing of personal information?	✔	✔	◑
2.	What is scope & coverage of privacy law?	Comprehensive	Comprehensive	Not applicable
3.	Is the privacy law compatible with the Privacy Principles in the EU Data Protection Directive?	✔	◑	✖
4.	Is the privacy law compatible with the Privacy Principles in the APEC Privacy Framework?	✔	✔	✖
5.	Is an independent private right of action available for breaches of data privacy?	Available	Not available	Available
6.	Is there an effective agency (or regulator) tasked with the enforcement of privacy laws?	National regulator	National regulator	None
7.	What is the nature of the privacy regulator?	Sole commissioner	Sole commissioner	Not applicable
8.	Are data controllers free from registration requirements?	✖	✔	✔
9.	Are cross-border transfers free from registration requirements?	◑	✔	✔
10.	Is there a breach notification law?	✖	✖	✖
	SECURITY			
1.	Is there a law or regulation that gives electronic signatures clear legal weight?	✔	✔	✔
2.	Are ISPs and content service providers free from mandatory filtering or censoring?	✔	✔	✔
3.	Are there laws or enforceable codes containing general security requirements for digital data hosting and cloud service providers?	Limited coverage in legislation	Limited coverage in legislation	None
4.	Are there laws or enforceable codes containing specific security audit requirements for digital data hosting and cloud service providers?	Limited coverage in legislation	None	None
5.	Are there security laws and regulations requiring specific certifications for technology products?	No requirements	Limited requirements	No requirements
	CYBERCRIME			
1.	Are cybercrime laws in place?	✔	✔	✖
2.	Are cybercrime laws consistent with the Budapest Convention on Cybercrime?	✔	✔	✖
3.	What access do law enforcement authorities have to encrypted data held or transmitted by data hosting providers, carriers or other service providers?	Access with a warrant	Access with a warrant	Access with a warrant
4.	How does the law deal with extraterritorial offenses?	Limited coverage	Comprehensive coverage	Comprehensive coverage
	INTELLECTUAL PROPERTY RIGHTS			
1.	Is the country a member of the TRIPS Agreement?	✔	✔	✔
2.	Have IP laws been enacted to implement TRIPS?	✔	✔	✔
3.	Is the country party to the WIPO Copyright Treaty?	✔	✔	✖
4.	Have laws implementing the WIPO Copyright Treaty been enacted?	◑	✔	◑
5.	Are civil sanctions available for unauthorized making available (posting) of copyright holders' works on the Internet?	◑	✔	◑
6.	Are criminal sanctions available for unauthorized making available (posting) of copyright holders' works on the Internet?	◑	✔	◑
7.	Are there laws governing ISP liability for content that infringes copyright?	✖	Undecided	✖
8.	Is there a basis for ISPs to be held liable for content that infringes copyright found on their sites or systems?	✖	✔	✖
9.	What sanctions are available for ISP liability for copyright infringing content found on their site or system?	Not applicable	Civil and criminal	Not applicable
10.	Must ISPs take down content that infringes copyright, upon notification by the right holder?	◑	✔	✖
11	Are ISPs required to inform subscribers upon receiving a notification that the subscriber is using the ISP's service to distribute content that infringes copyright?	✖	✔	✖
12.	Is there clear legal protection against misappropriation of cloud computing services, including effective enforcement?	Limited protection (criminal activity only)	Comprehensive protection	No protection
	SUPPORT FOR INDUSTRY-LED STANDARDS & INTERNATIONAL HARMONIZATION OF RULES			
1.	Are there laws, regulations or policies that establish a standards setting framework for interoperability and portability of data?	✖	✔	✖
2.	Is there a regulatory body responsible for standards development for the country?	✔	✔	✔
3.	Are e-commerce laws in place?	◑	✔	✖
4.	What international instruments are the e-commerce laws based on?	Not applicable	UNCITRAL Model Law on E-Commerce	Not applicable
5.	Is the downloading of applications or digital data from foreign cloud service providers free from tariff or other trade barriers?	✔	✔	✖
6.	Are international standards favored over domestic standards?	◑	✔	✔
7.	Does the government participate in international standards setting process?	✔	✔	✔



Canada	China	France	Germany	India	Indonesia	Italy
✔	✖	✔	✔	◑	◑	✔
Comprehensive	Not applicable	Comprehensive	Comprehensive	Sectoral	Comprehensive	Comprehensive
✔	✖	✔	✔	✖	✖	✔
✔	✖	✔	✔	✖	◑	✔
Available	Available	Available	Available	Available	Not available	Available
National regulator	None	National regulator	Sectoral regulator	None	None	National regulator
Sole commissioner	Not applicable	Sole commissioner	Sole commissioner	Not applicable	Not applicable	Collegial body
✔	✔	✖	✖	✔	✔	✖
✔	✔	✖	✔	◑	✔	✔
✖	✖	◑	◑	✖	✖	✖
✔	✔	✔	✔	✔	✔	✔
✔	✖	✔	◑	✖	◑	◑
None	None	Limited coverage in legislation	Limited coverage in legislation	Detailed legislation	None	Detailed legislation
Limited coverage in legislation	None	Limited coverage in legislation	None	Code of conduct	None	Limited coverage in legislation
Comprehensive requirements (including common criteria)	Limited requirements	Comprehensive requirements (including common criteria)	Comprehensive requirements (including common criteria)	Limited requirements	No requirements	Comprehensive requirements (including common criteria)
◑	✔	✔	✔	✔	✔	✔
◑	✖	✔	✔	✔	✔	✔
Access with a warrant	Not stated	Access with a warrant	Access with a warrant	Unlimited access	Not stated	Access with a warrant
Limited coverage	Limited coverage	Comprehensive coverage	Comprehensive coverage	Comprehensive coverage	Limited coverage	Limited coverage
✔	✔	✔	✔	✔	✔	✔
✔	◑	✔	✔	◑	◑	✔
✖	✔	✔	✔	✖	✔	✔
◑	◑	✔	✔	◑	◑	✔
◑	✔	✔	✔	✔	✔	✔
◑	✔	◑	◑	✔	✔	✔
Undecided	✔	✔	✔	◑	✖	✔
✖	✔	✔	◑	◑	Undecided	✔
Not applicable	Civil and criminal	Civil and criminal	Civil	Not applicable	Not applicable	Civil and criminal
✖	✔	✔	✔	✖	✖	◑
✖	✖	✔	✖	✖	✖	✖
Limited protection (criminal activity only)	Comprehensive protection	Comprehensive protection	Comprehensive protection	No protection	Comprehensive protection	Comprehensive protection
✔	✔	✔	✔	✔	✔	✔
✔	✔	✔	✔	✔	✔	✔
✔	✔	✔	✔	✔	✔	✔
UNCITRAL Model Law on E-Commerce	UN Convention on E-Contracting	UNCITRAL Model Law on E-Commerce	UNCITRAL Model Law on E-Commerce	UNCITRAL Model Law on E-Commerce	UN Convention on E-Contracting	UNCITRAL Model Law on E-Commerce
✔	◑	✔	✔	✔	✔	✔
✔	◑	✔	✔	✔	✔	✔
✔	✔	✔	✔	✔	✔	✔



Japan	Korea	Malaysia	Mexico	Poland	Russia	Singapore
✔	✔	✔	✔	✔	✔	✖
Comprehensive	Comprehensive	Sectoral	Comprehensive	Comprehensive	Comprehensive	Not applicable
◑	✔	◑	◑	✔	◑	✖
✔	✔	✔	◑	✔	✔	✖
Available	Available	Not available	Available	Available	Available	Not available
Sectoral regulator	National regulator	National regulator	National regulator	National regulator	National regulator	None
Other government official	Other government official	Sole commissioner	Collegial body	Sole commissioner	Other government official	Not applicable
✔	✔	✔	✔	✖	✖	✔
✔	✔	✔	✔	◑	✖	✔
◑	✔	✖	✔	◑	✔	✖
✔	✔	✔	✔	✔	✔	✔
✔	✖	✔	✔	✔	◑	✖
Limited coverage in legislation	Limited coverage in legislation	Limited coverage in legislation	Limited coverage in legislation	Limited coverage in legislation	Detailed legislation	None
Limited coverage in legislation	Limited coverage in legislation	None	None	None	None	None
Comprehensive requirements (including common criteria)	Limited requirements	Limited requirements	No requirements	Limited requirements	Comprehensive requirements	Limited requirements
✔	✔	✔	✔	✔	✔	✔
✔	✖	✖	✔	✔	◑	✔
Access with a warrant	Not stated	Undecided	Not stated	Not stated	Unlimited access	Access with a warrant
Comprehensive coverage	Comprehensive coverage	Comprehensive coverage	Limited coverage	Limited coverage	Limited coverage	Comprehensive coverage
✔	✔	✔	✔	✔	✖	✔
✔	✔	✔	✔	✔	◑	✔
✔	✔	✖	✔	✔	✔	✔
✔	✔	◑	◑	✔	✔	✔
✔	✔	✔	◑	✔	✖	✔
✔	✔	✔	◑	✔	✔	✔
✔	✔	✖	◑	✔	✖	✔
✔	✔	Undecided	◑	✔	✔	✔
Civil	Civil	Not applicable	Civil and criminal	Civil and criminal	Not applicable	Civil
✔	✔	✖	✖	✔	✖	✔
✔	✔	✖	✖	Undecided	✖	✔
Comprehensive protection	Comprehensive protection	Comprehensive protection	Limited protection (criminal activity only)	Comprehensive protection	Limited protection (criminal activity only)	Comprehensive protection
✔	✔	✔	✔	✔	✔	◑
✔	✔	✔	✔	✔	✔	✔
◑	✔	✔	✔	✔	◑	✔
Not applicable	UNCITRAL Model Law on E-Commerce	UN Convention on E-Contracting	UNCITRAL Model Law on E-Commerce	UNCITRAL Model Law on E-Commerce	UN Convention on E-Contracting	UN Convention on E-Contracting
✔	✔	✔	✔	✔	✔	✔
✔	◑	✔	✔	✔	◑	✔
✔	✔	✔	✔	✔	✔	✔

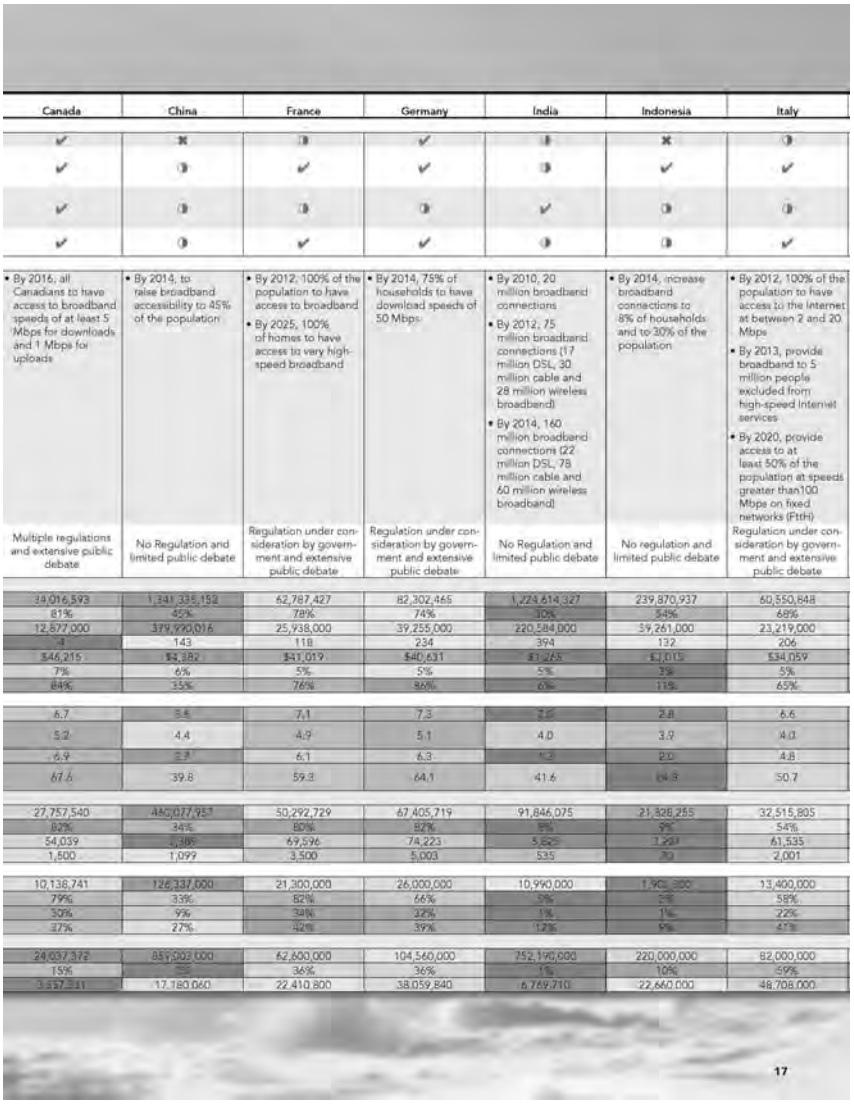


South Africa	Spain	Thailand	Turkey	United Kingdom	United States	Vietnam
✖	✔	✖	✖	✔	◑	◑
Not applicable	Comprehensive	Not applicable	Not applicable	Comprehensive	Sectoral	Not applicable
✖	✔	✖	✖	✔	✖	✖
✖	✔	✖	✖	✔	◑	✖
Available	Available	Available	Available	Available	Available	Undecided
None	National regulator	None	None	National regulator	Sectoral regulator	None
Not applicable	Sole commissioner	Not applicable	Not applicable	Sole commissioner	Other government official	Not applicable
✔	✖	✔	✔	✖	✔	✔
✔	✖	✔	✔	✔	◑	✔
✖	◑	✖	✖	◑	✔	✖
✔	✔	✔	✔	✔	✔	✔
◑	✔	✖	✖	✔	✔	✖
None	Limited coverage in legislation	None	None	Limited coverage in legislation	Limited coverage in legislation	Limited coverage in legislation
None	None	None	None	Limited coverage in legislation	Limited coverage in legislation	None
No requirements	Comprehensive requirements (including common criteria)	No requirements	Comprehensive requirements (including common criteria)	Comprehensive requirements (including common criteria)	Comprehensive requirements (including common criteria)	No requirements
✔	✔	✔	✔	✔	✔	✔
✔	✔	✔	◑	◑	✔	✖
Access with a warrant	No access	Unlimited access	Not stated	Unlimited access	Not stated	Unlimited access
Comprehensive coverage	Comprehensive coverage	Comprehensive coverage	Limited coverage	Comprehensive coverage	Limited coverage	Limited coverage
✔	✔	✔	✔	✔	✔	✔
✔	✔	◑	✔	✔	✔	◑
✖	✔	✖	✔	✔	✔	✖
◑	✔	✖	✔	✔	✔	◑
✔	◑	✔	✔	✔	Undecided	✔
✔	◑	✔	Undecided	✔	Undecided	✔
✔	✔	✖	✔	✔	✔	✖
✔	✔	✖	✔	✔	✔	✖
Civil	Civil	Not applicable	Civil and criminal	Civil and criminal	Civil and criminal	Not applicable
✔	✔	✖	✔	✖	✔	✖
✖	✖	✖	✖	◑	◑	✖
Comprehensive protection	Comprehensive protection	No protection	Comprehensive protection	Comprehensive protection	Comprehensive protection	No protection
✔	✔	✔	✔	✔	✔	✔
✔	✔	✔	✔	✔	✔	✔
✔	✔	✔	◑	✔	✔	✔
UNCITRAL Model Law on E-Commerce	UNCITRAL Model Law on E-Commerce	UNCITRAL Model Law on E-Commerce	Other	Other	Other	UNCITRAL Model Law on E-Commerce
✔	✔	✔	✔	✔	✔	✖
✔	✔	✔	✔	✔	✔	◑
✔	✔	✔	✔	✔	✔	✔

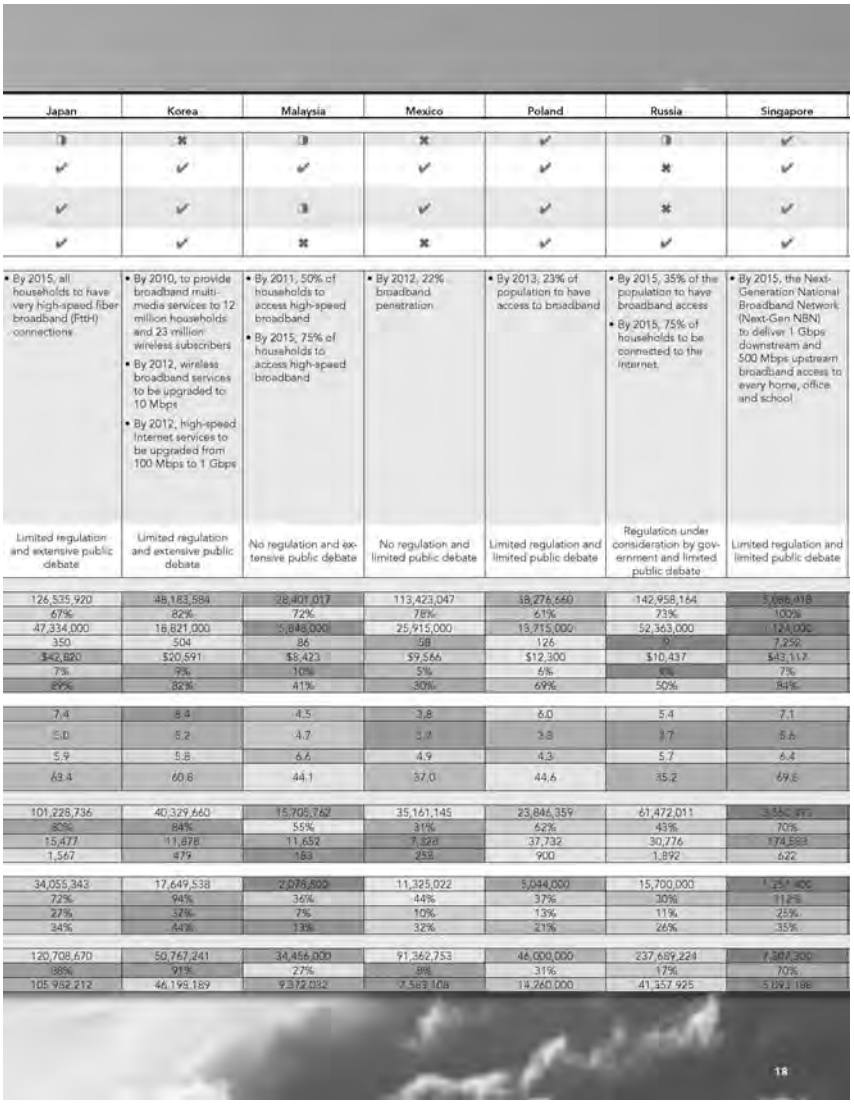
# QUESTION	Argentina	Australia	Brazil
PROMOTING FREE TRADE			
1. Are any laws or policies in place that implement technology neutrality in government?	✖	✔	✖
2. Are cloud computing services able to operate free from laws or policies that mandate the use of certain products (including, but not limited to types of software), services, standards or technologies?	✔	✔	✔
3. Are cloud computing services able to operate free from laws or policies that establish preferences for certain products (including, but not limited to types of software), services, standards, or technologies?	✔	✔	◑
4. Are cloud computing services able to operate free from laws that discriminate based on the nationality of the vendor, developer or service provider?	◑	◑	✖
ICT READINESS, BROADBAND DEPLOYMENT			
1. Is there a National Broadband Plan?	• By 2015, more than 10 million homes with broadband access	• By 2021, the National Broadband Network (NBN) will cover 100% of premises, 93% of homes, schools and businesses at up to 100 Mbps over fiber, with the remainder at up to 12 Mbps over next-generation wireless and satellite	• By 2014, 30 million fixed broadband connections (with a minimum speed of 1Mbps), including homes, businesses and co-operatives, plus 100,000 telecenters
2. Are there laws or policies that regulate the establishment of different service levels for data transmission based on the nature of data transmitted?	Limited regulation and limited public debate	No regulation and extensive public debate	Regulation under consideration by government and extensive public debate
3. Base Indicators			
3.1. Population (2010)	40,412,376	22,348,834	194,946,470
3.2. Urban Population (%) (2010)	92%	89%	87%
3.3. Number of Households (2009)	10,960,000	8,400,000	57,650,000
3.4. Population Density (people per square km) (2010)	15	3	23
3.5. Per Capita GDP (USD 2010)	$9,138	$39,990	$10,816
3.6. ICT Expenditure as % of GDP (2008)	5%	5%	5%
3.7. Personal Computers (% of households) (2010)	40%	71%	35%
4. ICT and Network Readiness Indicators			
4.1. ITU ICT Development Index (IDI) (2010) *(Score is out of 10 and includes 152 countries)*	4.6	7.4	4.3
4.2. World Economic Forum Networked Readiness Index (2010–2011) *(Score is out of 7 and includes 138 countries)*	3.5	5.1	3.9
4.3. International Connectivity Score (2011) *(Score is out of 10 and includes 50 countries)*	5.5	6.9	5.1
4.4. IT Industry Competitiveness Index (2011) *(Score is out of 100 and includes 66 countries)*	38.2	67.5	39.5
5. Internet Users and International Bandwidth			
5.1. Internet Users (2010)	14,548,455	16,235,572	79,343,213
5.2. Internet Users as % of Population (2010)	36%	76%	41%
5.3. International Internet Bandwidth (bits per second per Internet user) (2010)	27,494	41,361	12,819
5.4. International Internet Bandwidth (2010) (total gigabits per second (Gbps) per country)	400	700	1,001
6. Fixed Broadband			
6.1. Fixed Broadband Subscriptions (2010)	3,952,395	5,166,000	14,086,729
6.2. Fixed Broadband Subscriptions as % of households (2010)	35%	61%	24%
6.3. Fixed Broadband Subscriptions as % of population (2010)	10%	23%	7%
6.4. Fixed Broadband Subscriptions as % of Internet users (2010)	27%	31%	18%
7. Mobile Broadband			
7.1. Mobile Cellular Subscriptions (2010)	57,300,000	23,580,500	202,944,033
7.2. Active Mobile-broadband Subscriptions per 100 inhabitants (2010)	13%	83%	11%
7.3. Number of Active Mobile-broadband Subscriptions per 100 inhabitants (2010)	5,034,400	18,607,500	21,512,067

ICT Readiness (Country Ranking Out of 24)

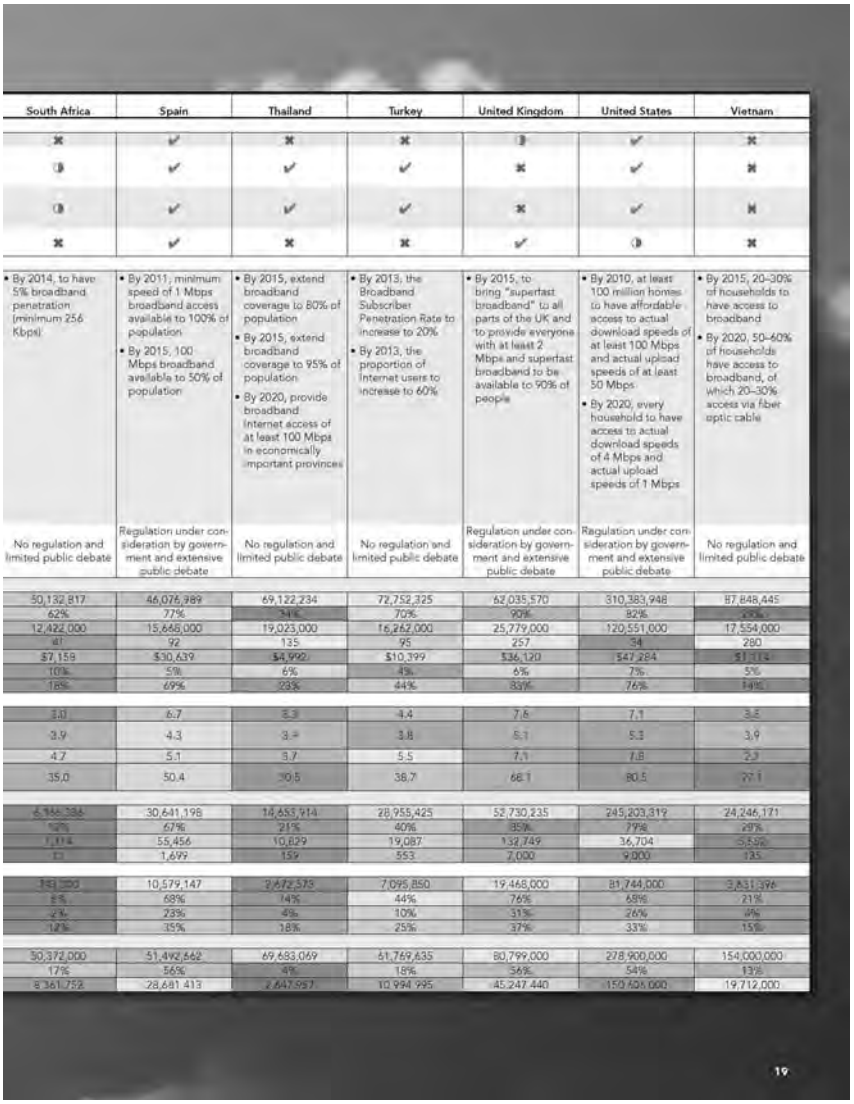
Highest — Lowest



Canada	China	France	Germany	India	Indonesia	Italy
✔	✖	◑	✔	◑	✖	◑
✔	◑	✔	✔	◑	✔	✔
✔	◑	◑	◑	✔	◑	◑
✔	◑	✔	✔	◑	◑	✔
• By 2016, all Canadians to have access to broadband speeds of at least 5 Mbps for downloads and 1 Mbps for uploads	• By 2014, to raise broadband accessibility to 45% of the population	• By 2012, 100% of the population to have access to broadband • By 2025, 100% of homes to have access to very high-speed broadband	• By 2014, 75% of households to have download speeds of 50 Mbps	• By 2010, 20 million broadband connections • By 2012, 75 million broadband connections (17 million DSL, 30 million cable and 28 million wireless broadband) • By 2014, 160 million broadband connections (22 million DSL, 78 million cable and 60 million wireless broadband)	• By 2014, increase broadband connections to 8% of households and to 30% of the population	• By 2012, 100% of the population to have access to the Internet at between 2 and 20 Mbps • By 2013, provide broadband to 5 million people excluded from high-speed Internet services • By 2020, provide access to at least 50% of the population at speeds greater than100 Mbps on fixed networks (FttH)
Multiple regulations and extensive public debate	No Regulation and limited public debate	Regulation under consideration by government and extensive public debate	Regulation under consideration by government and extensive public debate	No Regulation and limited public debate	No regulation and limited public debate	Regulation under consideration by government and extensive public debate
34,016,593	1,341,335,152	62,787,427	82,302,465	1,224,614,327	239,870,937	60,550,848
81%	45%	78%	74%	30%	54%	68%
12,877,000	379,990,016	25,938,000	37,255,000	220,584,000	59,261,000	23,219,000
4	143	118	234	394	132	206
$46,215	$4,382	$41,019	$40,631	$1,265	$2,015	$34,059
7%	6%	5%	5%	5%	3%	5%
84%	35%	76%	86%	6%	11%	65%
6.7	3.6	7.1	7.3	2.5	2.8	6.6
5.2	4.4	4.9	5.1	4.0	3.9	4.0
6.9	2.7	6.1	6.3	1.3	2.0	4.8
67.6	39.8	59.3	64.1	41.6	64.9	50.7
27,757,540	440,077,951	50,292,729	67,405,719	91,846,075	21,326,255	32,515,805
82%	34%	80%	82%	8%	9%	54%
54,039	3,386	69,596	74,223	5,625	1,293	61,535
1,500	1,099	3,500	5,003	535	70	2,001
10,138,741	126,337,000	21,300,000	26,000,000	10,990,000	1,900,000	13,400,000
79%	33%	82%	66%	5%	5%	58%
30%	9%	34%	32%	1%	1%	22%
37%	27%	42%	39%	12%	9%	47%
24,037,372	857,003,000	62,600,000	104,560,000	752,190,000	220,000,000	82,000,000
15%	7%	36%	36%	1%	10%	59%
3,557,311	17,780,060	22,410,800	38,059,840	6,769,710	22,660,000	48,708,000



Japan	Korea	Malaysia	Mexico	Poland	Russia	Singapore
◑	✖	◑	✖	✔	◑	✔
✔	✔	✔	✔	✔	✖	✔
✔	✔	◑	✔	✔	✖	✔
✔	✔	✖	✖	✔	✔	✔
• By 2015, all households to have very high-speed fiber broadband (FttH) connections	• By 2010, to provide broadband multimedia services to 12 million households and 23 million wireless subscribers • By 2012, wireless broadband services to be upgraded to 10 Mbps • By 2012, high-speed Internet services to be upgraded from 100 Mbps to 1 Gbps	• By 2011, 50% of households to access high-speed broadband • By 2015, 75% of households to access high-speed broadband	• By 2012, 22% broadband penetration	• By 2013, 23% of population to have access to broadband	• By 2015, 35% of the population to have broadband access • By 2015, 75% of households to be connected to the Internet	• By 2015, the Next-Generation National Broadband Network (Next-Gen NBN) to deliver 1 Gbps downstream and 500 Mbps upstream broadband access to every home, office and school
Limited regulation and extensive public debate	Limited regulation and extensive public debate	No regulation and extensive public debate	No regulation and limited public debate	Limited regulation and limited public debate	Regulation under consideration by government and limited public debate	Limited regulation and limited public debate
126,535,920	48,183,584	28,401,017	113,423,047	38,276,660	142,958,164	5,686,418
67%	82%	72%	78%	61%	73%	100%
47,334,000	18,821,000	5,848,000	25,915,000	13,715,000	52,363,000	124,000
350	504	86	58	126	0	7,250
$42,820	$20,591	$8,423	$9,566	$12,300	$10,437	$43,117
7%	9%	10%	5%	6%	6%	7%
89%	82%	41%	30%	69%	50%	84%
7.4	8.4	4.5	3.8	6.0	5.4	7.1
5.0	5.2	4.7	3.9	3.8	3.7	5.6
5.9	5.8	6.6	4.9	4.3	5.7	6.4
63.4	60.6	44.1	37.0	44.6	35.2	69.6
101,228,736	40,329,660	15,705,762	35,161,145	23,846,359	61,472,011	3,886,491
80%	84%	55%	31%	62%	43%	70%
15,477	11,678	11,652	7,328	37,732	30,776	174,583
1,567	479	183	258	900	1,892	622
34,055,343	17,649,538	2,076,600	11,325,022	5,044,000	15,700,000	1,251,400
72%	94%	36%	44%	37%	30%	112%
27%	37%	7%	10%	13%	11%	23%
34%	44%	13%	32%	21%	26%	35%
120,708,670	50,767,241	34,466,000	91,362,753	46,000,000	237,689,224	7,387,300
98%	91%	27%	8%	31%	17%	70%
105,982,212	46,199,189	9,372,092	7,583,108	14,260,000	41,357,925	5,093,198



South Africa	Spain	Thailand	Turkey	United Kingdom	United States	Vietnam
✖	✔	✖	✖	◑	✔	✖
◑	✔	✔	✔	✖	✔	✖
◑	✔	✔	✔	✖	✔	✖
✖	✔	✖	✖	✔	◑	✖
• By 2014, to have 5% broadband penetration (minimum 256 Kbps)	• By 2011, minimum speed of 1 Mbps broadband access available to 100% of population • By 2015, 100 Mbps broadband available to 50% of population	• By 2015, extend broadband coverage to 80% of population • By 2015, extend broadband coverage to 95% of population • By 2020, provide broadband Internet access of at least 100 Mbps in economically important provinces	• By 2013, the Broadband Subscriber Penetration Rate to increase to 20% • By 2013, the proportion of Internet users to increase to 60%	• By 2015, to bring "superfast broadband" to all parts of the UK and to provide everyone with at least 2 Mbps and superfast broadband to be available to 90% of people	• By 2010, at least 100 million homes to have affordable access to actual download speeds of at least 100 Mbps and actual upload speeds of at least 50 Mbps • By 2020, every household to have access to actual download speeds of 4 Mbps and actual upload speeds of 1 Mbps	• By 2015, 20–30% of households to have access to broadband • By 2020, 50–60% of households have access to broadband, of which 20–30% access via fiber optic cable
No regulation and limited public debate	Regulation under consideration by government and extensive public debate	No regulation and limited public debate	No regulation and limited public debate	Regulation under consideration by government and extensive public debate	Regulation under consideration by government and extensive public debate	No regulation and limited public debate
50,132,817	46,076,989	69,122,234	72,752,325	62,035,570	310,383,948	87,848,445
62%	77%	34%	70%	90%	82%	29%
12,422,000	15,646,000	19,023,000	16,262,000	25,779,000	120,551,000	17,554,000
41	92	135	95	257	34	280
$7,159	$30,639	$4,992	$10,399	$36,120	$47,284	$1,314
10%	5%	6%	4%	6%	7%	5%
18%	69%	23%	44%	83%	76%	14%
3.0	6.7	8.3	4.4	7.6	7.1	3.5
3.9	4.3	3.9	3.8	5.1	5.3	3.9
4.7	5.1	3.7	5.5	7.1	7.8	2.3
35.0	50.4	30.5	38.7	68.1	80.5	22.1
8,346,384	30,641,198	14,453,914	28,955,425	52,730,235	245,203,319	24,246,171
16%	67%	21%	40%	85%	79%	28%
1,114	55,456	10,829	19,087	132,749	36,704	3,556
13	1,699	159	553	7,000	9,000	135
351,200	10,579,147	2,672,575	7,095,850	19,468,000	81,744,000	3,831,396
8%	68%	14%	44%	76%	68%	21%
2%	23%	4%	10%	31%	26%	4%
12%	35%	18%	25%	37%	33%	15%
50,372,000	51,492,662	69,683,069	61,769,635	80,799,000	278,900,000	154,000,000
17%	56%	4%	18%	56%	54%	13%
8,361,752	28,681,413	2,647,957	10,994,995	45,247,440	150,606,000	19,712,000

ABOUT BSA

The Business Software Alliance (BSA) is the leading advocate for the global software industry before governments and in the international marketplace. It is an association of world-class companies that invest billions of dollars annually to create software solutions that spark the economy and improve modern life.

BSA serves as the world's premier anti-piracy organization and as a respected leader in shaping public policies that promote technology innovation and drive economic growth.

Through government relations, intellectual property enforcement and educational activities in markets around the world, BSA protects intellectual property and fosters innovation; works to open markets and ensure fair competition; and builds trust and confidence in information technology for consumers, businesses and governments alike.

PROTECTING INTELLECTUAL PROPERTY & FOSTERING INNOVATION

Intellectual property rights (IPR) — copyrights, patents and trademarks — provide the legal framework for creative enterprise, the bedrock of growing economies. They are also essential to commercial software development, which is the world's largest copyright industry.

By working with policymakers, leading enforcement actions and conducting public-education initiatives around the world, BSA ensures that respect for IPR pervades the global economy and society.

- Championing Intellectual Property Rights: BSA works with governments around the world to ensure intellectual property protections keep pace with new innovations in technology, such as cloud computing.
- Curbing Software Theft: BSA conducts vigorous enforcement programs in approximately 50 countries, helping its members guard against software theft by taking legal action against commercial, end-user license infringement, counterfeiting operations and Internet piracy.
- Leading Industry Research: BSA publishes the most authoritative global studies on piracy and its economic impact, illuminating the scope of the problem and helping shape national and international policy responses.
- Educating the Public: BSA educates consumers about harms associated with software piracy and offers a groundbreaking training program to help organizations more effectively manage their software assets.

BSA serves as the world's premier anti-piracy organization and as a respected leader in shaping public policies that promote technology innovation and drive economic growth.

OPENING MARKETS & ENSURING FAIR COMPETITION

Open markets are essential to economic growth and prosperity. BSA expands market opportunities for the software industry by working with governments to break down trade barriers and eliminate discriminatory procurement preferences that stifle innovation by skewing competition.

- Breaking Down Barriers to Growth: BSA provides policymakers with information, expert analysis and industry insights to promote an open-markets agenda. These efforts include a special focus on the so-called 'BRIC' economies of Brazil, Russia, India and China, which are the world's fastest-growing technology markets but also home to rampant piracy.
- Promoting Technology Neutrality: BSA encourages fair competition among technologies by promoting internationally recognized standards and unbiased IT-procurement policies for governments.
- Supporting New Innovations: BSA works with policymakers around the world to create conditions for new technologies, such as cloud computing, to flourish. In addition to collaborating on technology standards, this work involves elevating intellectual property protections, harmonizing international legal principles and addressing other challenges that are beyond the capability or jurisdiction of any one company or government.

BUILDING TRUST & CONFIDENCE IN TECHNOLOGY

Security and privacy undergird trust and confidence in information technology for consumers, businesses and governments. BSA promotes responsible data stewardship and facilitates acceptance and adoption of each new wave of innovation that transforms the technology marketplace and creates value for society.

- Driving Public-Private Collaboration: Drawing on the expertise of its members and productive working relationships with public officials, BSA serves as a knowledge center and catalyst to encourage cooperation and forge consensus among industry and governments.
- Protecting Consumers: As new technologies emerge, such as cloud computing, BSA and its members develop appropriate privacy and security standards and share their insights with policymakers and regulators.
- Mapping Policy Solutions: BSA has developed a global cybersecurity framework to guide governments in crafting policies that effectively deter and punish cyber crime, mitigate threats, inform and protect consumers, and respond to cyber incidents.


BSA.
BUSINESS SOFTWARE ALLIANCE
www.bsa.org
BSA Worldwide Headquarters
1150 18th Street, NW
Suite 700
Washington, DC 20036
T: +1.202.872.5500
F: +1.202.872.5501
BSA Asia-Pacific
300 Beach Road
#25-08 The Concourse
Singapore 199555
T: +65.6292.2072
F: +65.6292.6369
BSA Europe, Middle East & Africa
2 Queen Anne's Gate Buildings
Dartmouth Street
London, SW1H 9BP
United Kingdom
T: +44.207.340.6080
F: +44.207.340.6090
Bangkok, Thailand Beijing, China Brussels, Belgium Hanoi, Vietnam Jakarta, Indonesia Kuala Lumpur, Malaysia
München, Germany New Delhi, India São Paulo, Brazil Taipei, Taiwan Tokyo, Japan

TechAmerica
FOUNDATION

Cloud First, Cloud Fast:

Recommendations for Innovation, Leadership and Job Creation



A Report from the Commission on the Leadership Opportunity in U.S. Deployment of the Cloud (CLOUD^2)

Commission on the Leadership Opportunity in U.S. Deployment of the Cloud (CLOUD^2)

Leadership

Marc Benioff (Co-Chair)
Salesforce.com

Michael Capellas (Co-Chair)
VCE

John Mallery (Academic Co-Chair)
MIT

Michael R. Nelson (Academic Co-Chair)
Georgetown University

Jim Sheaffer (Vice Chair, Public Sector)
CSC

Dan Reed (Vice Chair, Commercial)
Microsoft

Commissioners

Stephen Alexander
Cinna Corporation

JP Balakrishnan
Infosys

Ashok Balasubramanian
Syntel

Greg Baroni
Attain, LLC

Kia Behnia
BMC Software

Jeff Bergeron
HP Enterprise Services

Evan Burfield
Synteractive

Juan Carlos Soto
Informatica Corporation

Teresa H. Carlson
Amazon, AWS

Alan Chow
Teradata Corporation

Keith Collins
SAS

Lance Crosby
SoftLayer Technologies

Peter D. Csathy
Sorenson Media, Inc.

Alan Davidson
Google, Inc.

William A Davies
Research In Motion, Limited

Adam Famularo
CA Technologies

Gregory Gardner
NetApp

Greg Gianforte
RightNow Technologies

Keith Glennan
Northrop Grumman Corporation

Diana L. Gowen
Qwest Government Services, Inc.

Phil Horvitz
URS-Apptis

Paul W. Hurley
Securicon

Michael Isman
Booz Allen Hamilton

Richard W. Johnson
Lockheed Martin IS&GS

Wolfgang Kandek
Qualys

Daniel Kent
Cisco Systems, Inc.

Barry Leffew
Adobe

Robin Lineberger
Deloitte LLP

Albert Lulushi
L-3 Communications

Brad Maltz
International Computerware, Inc.

Eric Marks
AgilePath Corporation

Timothy Matlack
Delta Solutions and Technologies, Inc.

Daniel Matthews
Information Innovators, Inc.

Nick Mehta
LiveOffice

Lew Moorman
Rackspace Hosting, Inc.

Gregg Mossburg
CGI Federal

Ray Muslimani
GCE

Jeff Nick
EMC Corporation

Steven Perkins
Grant Thornton

Edward M.L. Peters
OpenConnect

Sterling Phillips
GTSI Corporation

Sanjay Poonen
SAP AG

John Potter
AT&T Business Solutions

Branko Primetica
eGlobalTech

Todd Ramsey
IBM Corporation

Jim Reavis
Cloud Security Alliance

Kurt Roemer
Citrix

David M. Shacochis
Savvis

Suresh Shenoy
INC, Inc.

Steve Siske
Serco North America

James 'Bo' Slaughter
SRA International

Wyatt Starnes
Harris Corporation

Ken Stephens
ACS, A Xerox Company

Dave Stevens
Brocade Communications, Inc.

Grady Summers
Ernst & Young

Stanley Tyliszczak
General Dynamics Information Technology

Michael Van Chau
MEI Technologies, Inc.

Doug Wagoner
SAIC

John Weinschenk
Genzic, Inc.

Teresa A. Weipert
Accenture

James "Rick" White
Wyle Information Systems

Jim Whitehurst
Red Hat, Inc.

Bernie Wu
FalconStor Software

Susan Zeleniak
Verizon Business

Hemi Zucker
j2 Global Communications, Inc.

CLOUD^2 Staff Directors

Jennifer A. Kerber
Staff Director,
TechAmerica Foundation

Christopher E. Wilson
Deputy Staff Director,
TechAmerica Foundation

CLOUD^2 COMMISSION REPORT

Foreword

Cloud technologies are transforming the way computing power is bought, sold and delivered. Rather than purchasing licenses or hardware, users may now obtain computing power as a service, buying only as much as they need, and only when they need it. This new business model brings vast efficiency and cost advantages to government agencies, individuals, and companies of all sizes. The numerous benefits of cloud computing have already won over many adopters and are generating significant cost savings, efficiencies, flexibility, innovation, and new market opportunities.

This report reflects the growing imperative to fully embrace and capitalize upon the power of cloud computing. The Commission on the Leadership Opportunity in U.S. Deployment of the Cloud (CLOUD^2) developed the report at the encouragement of the Federal Chief Information Officer and the U.S. Department of Commerce. The Commission's mandate was to generate recommendations for accelerating adoption of cloud technologies in the U.S. government and in the commercial space and to identify public policies that will help foster U.S. innovation and leadership in cloud computing.

The Commission was composed of representatives from 71 companies and organizations, including cloud providers, cloud users, and other businesses that are involved in enabling cloud deployment. To build on this diverse set of expertise and perspectives, the Commissioners interviewed numerous government representatives, heard presentations from a variety of organizations, and analyzed relevant past reports.



Actionable Recommendations — Trust, Transnational Data Flows, Transparency and Transformation

Moving to cloud computing is a change that involves people, policies, processes, and technology. The Commission identified barriers that have kept some government agencies from moving to the cloud and recommended actionable solutions to overcome these. In addition, the Commission identified barriers to commercial deployment of cloud services and recommended actions to eliminate them. Since government, industry and academia share the responsibility to accelerate adoption and drive U.S. innovation and leadership, the recommendations reflect actions for all three key stakeholders. Industry, as represented by the Commission members, is committed to enabling the transition to the cloud by companies and government agencies and accepts the responsibility for taking actions that enable cloud adoption.

In this report, the Commission has focused on 14 specific recommendations, categorized into four thematic areas: Trust, Transnational Data Flows, Transparency, and Transformation. For each recommendation, the report identifies why the action is needed, how it should be implemented, who should implement it, and what benefits should be expected from implementation. The Commission intentionally made these recommendations direct and prescriptive.

The four areas are briefly discussed below.

Trust
Users of cloud computing want assurance that when using cloud services, their workloads and data will be treated with the highest integrity and their security, privacy, and availability needs will be met. To enable trust and confidence in cloud services, the Commission recommends that government and industry develop common frameworks, best practices and metrics around security and information assurance to assist users in choosing and deploying the security level most appropriate for their workloads. The Commission also recommends strengthening the identity management ecosystem and data breach laws, as well as supporting increased research on cloud computing as an investment in future cloud innovation.

Transnational Data Flows
In a global economy, it is common for businesses to operate in multiple countries and for cloud providers and users to work and transfer information across national borders. This adds complexity to cloud adoption because of the data, processes, and people residing on multiple continents with different laws and cultures. In this context, the Commission recommends that industry and the U.S. government promote privacy frameworks, that the U.S. government identify and implement mechanisms to clarify processes and mechanisms around lawful government access to data, and that the U.S. continue international

discussions in these areas. We also recommend that the U.S. government lead by example by demonstrating its willingness to trust cloud computing environments in other countries for appropriate government workloads.

Transparency

Users want an abundance of information about the cloud services they buy and unfettered access to the data and processes they entrust to the service provider. To meet these needs, cloud providers must be open and transparent regarding the characteristics and operations of the services they provide. Government and industry should collaboratively develop metrics that facilitate this information sharing and customers' ability to compare cloud offerings. Additionally, to ensure that data is available to customers should they wish to change cloud providers, cloud providers should enable portability through industry standards and best practices.

Transformation

The transition to cloud computing is placing new requirements on purchasing processes, infrastructure, and people's skills. For government agencies, the fact that buying cloud computing services can be fundamentally different from buying in-house IT systems poses a challenge. Therefore, agencies, the Office of Management and Budget (OMB), and Congress must demonstrate more flexibility around budgeting and acquisition processes. Such flexibility, in combination with OMB incentives for moving to the cloud, will increase the rate of adoption by government agencies. Additionally, to accommodate the bandwidth and reliable connectivity necessary for the growth of cloud computing, the nation's currently stretched and aging IT broadband infrastructure should be updated, in conjunction with embracing IPv6. To help acquisition and IT personnel understand and carry out the transition to cloud, government agencies, companies, and academia should develop and disseminate appropriate educational resources.

> *"To do more with less, we need game-changing technologies. Cloud computing is one such technology."*
>
> -Vivek Kundra
> Federal CIO
>
> Testimony before the House Oversight and Government Reform Subcommittee on Government Management, Organization, and Procurement (July 1, 2010)

In addition to the recommendations in the body of the report, the Commission also produced the *Cloud Buyer's Guide*. The guide walks potential government buyers through questions to ask and steps to take prior to purchasing a cloud computing solution. Designed to be a living document, the guide is available online at http://www.cloudbuyersguide.org/. As cloud technology evolves, this online resource can be easily updated with new frequently asked questions (FAQs) and guidance.

By providing clear, actionable recommendations, the Commission hopes to help accelerate the deployment of cloud computing at companies and government agencies. Cloud's widespread adoption will drive increased efficiencies and job growth and continue to position the United States as a technology leader in a global marketplace.

Table of Contents

Foreword	**1**
Introduction	**5**
Trust	**8**
Recommendation 1 (Security & Assurance Frameworks)	9
Recommendation 2 (Identity Management)	10
Recommendation 3 (Responses to Data Breaches)	12
Recommendation 4 (Research)	12
Transnational Data Flows	**14**
Recommendation 5 (Privacy)	15
Recommendation 6 (Government/Law Enforcement Access to Data)	15
Recommendation 7 (E-Discovery and Forensics)	16
Recommendation 8 (Lead by Example)	17
Transparency	**19**
Recommendation 9 (Transparency)	20
Recommendation 10 (Data Portability)	20
Transformation	**22**
Recommendation 11 (Federal Acquisition and Budgeting)	23
Recommendation 12 (Incentives)	24
Recommendation 13 (Improve Infrastructure)	25
Recommendation 14 (Education/Training)	26
Conclusion	**27**
Recommendations	**28**
Acknowledgements	**31**

Introduction

For more than 50 years, the United States has taken advantage of new developments in Information Technology (IT). U.S. companies and government agencies were early adopters of the mainframe computer, the minicomputer, the personal computer, and the World Wide Web. We are now entering a new phase in the history of computing that will be at least as transformative as the mainframe or the Web and provide at least as much benefit to all Americans. Cloud computing represents a powerful new way to provide computing power and storage—and it will unleash huge new opportunities for companies and citizens able to harness it.

Cloud computing[1] is based on a simple idea. By allowing computer users to tap into servers and storage systems scattered around the country and around the world—and tied together by the Internet—cloud service providers can give users better, more reliable, more affordable, and more flexible access to the IT infrastructure they need to run their businesses, organize their personal lives, or obtain services ranging from entertainment to education, e-government, and healthcare. Most Americans already use cloud computing in one form or another to do email or back up the files on their laptop or smartphone. Most social networking sites and thousands of e-commerce sites (large and small) are running in the cloud. Cloud computing is not a technology of the future; it is already being used for business and government applications worldwide.

On the other hand, cloud computing does represent a fundamental shift in how computing is accomplished. The cloud is not only a new way to more easily and cheaply get the computing power needed to do what companies and individuals are doing today; the cloud, like the Web, will also generate new business models and drive companies to reorganize and change the way they go to market, team with partners, and serve their customers. It will enable companies (and governments) to move faster and be more responsive and flexible.

Companies will be able to try several prototypes at once, test their limits, and then build and deploy new, better prototypes—all within a few weeks. This may be the most important benefit of the cloud—it enables companies of all sizes and in all sectors, as well as governments, non-profits, and individuals, to more quickly build new applications and services by reducing the cost and complexity of deploying and managing IT resources. However, that requires cloud providers to make services simple and easy to use and deploy, and it requires that cloud customers make the effort to understand the new capabilities clouds can provide. Most companies and organizations spend the vast majority of their IT budget just maintaining

---

[1] The National Institute of Standards and Technology, in consultation with industry and government, has drafted a definition of cloud, including descriptions of the essential characteristics, service models, and deployment models See http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

their current infrastructures and the applications that run on them. The cloud will enable them to devote more resources and talent to creating new products and services and improving productivity.

This democratization of innovation is a huge opportunity for people, organizations, and countries around the world. To maintain its competitive position, the United States must focus on quickly and effectively harnessing the full power of cloud computing, leading in both the deployment of cloud and the development of new cloud services. This will help American companies generate high-paying jobs and compete in the global marketplace.

Whether the United States will benefit as much from this new phase in the evolution of computing as it did from the mainframe and the Web depends upon many factors. Will the iconic U.S. companies that have pioneered and promoted the cloud continue to lead in the development of cloud services? Will companies embrace cloud computing and take advantage of the capabilities it provides? Will the public sector be able to move to the cloud? Will individuals be comfortable with their data and software located in the cloud rather than on a device in their hand? Will government policies—both in the United States and abroad—facilitate deployment of and innovation in cloud services? We firmly believe that the answer to all these questions can and should be an unequivocal YES.

We are convinced that cloud computing is developing extremely rapidly, much like the Web did in the 1990s, and will have a major impact on computing and the economy. How cloud computing develops will be shaped by key choices and policy decisions that will be made over the next two or three years. It is critical that industry and government work together to make the right choices.

> *"This feels like 1997 for the Internet. People are asking the same questions about the cloud today that they did about the Internet back in 1997."*
>
> -Technology Strategist
> Software Company
>
> Quote from Sandhill Group
> Leaders in the Cloud
> K. Pennaraju, M.R. Rangswami
> (March 2010), p-13

In some cases, the U.S. government may choose NOT to take action and allow market forces to guide the evolution of the digital economy. U.S. national policies that conflict with those of other countries, even if designed to achieve worthy goals like security or consumer protection, could end up constraining how the cloud develops or discouraging investment in new cloud services and applications.

The most effective way for governments to shape the evolution of the cloud is not through law and regulation but by being smart users of the technology. This is particularly true in the area of security, where some government agencies have especially challenging requirements. As agencies work with industry to ensure that the cloud services deployed are at least as secure and trusted as the IT systems in use today, the agencies can provide a model that cloud customers in governments and corporations around the world can emulate.

This report provides recommendations for how government, including the White House and key federal agencies, in cooperation with industry, academia, and other nations, can (1) adopt policies that will foster development and growth of the cloud and (2) deploy the cloud effectively, making government work better, cheaper, and smarter. These recommendations cover a lot of territory but focus on four areas: Trust, Transnational Data Flows, Transparency, and Transformation. Responsibility for success also lies with cloud providers, and the Commission makes specific recommendations to providers throughout the report. The report also includes a "Buyer's Guide" that advises federal agencies on how to accelerate adoption of cloud services.



TRUST

The first step in accelerating the adoption of the cloud and driving U.S. leadership in cloud innovation is earning the trust of current and potential cloud users. Trust in the cloud is a result of a combination of factors that enable individuals and organizations consuming cloud services to be confident that the services are meeting their computing needs. These needs include security, privacy, and availability; the factors that contribute include transparency of practices, accountability, resiliency and redundancy, access and connectivity, supply chain provenance, life cycle integrity, and governance.

Cloud computing is the natural evolution of IT, and it will continue to evolve. Similarly, enabling trust in the cloud is an evolution—trust is not a static state, and cloud services are not static deployments. As cloud computing evolves, one element that will enable trust is the monitoring of characteristics that impact the quality of cloud service delivery and continuity. Monitoring can expose what is happening in a cloud deployment, and, coupled with systems for analysis, improvement, and accountability, can help enable trust in the functioning and security of the cloud.

Risk management is an important element of enabling trust because it is integral to the process of monitoring and accelerating cloud adoption and implementation in the short term. Risk management capabilities need improvement for enterprises adopting cloud services, for communications providers connecting cloud services to people, for cloud service providers, and for application providers. Areas relevant to the cloud include review of current and emerging standards, industry best practices, understanding risk simultaneously at a system level and asset level, risk transfer in cyberspace, methods for assessing and meeting security needs of data whose sensitivity varies over time, and mitigation of abuse of cloud assets.

This Commission believes that trust is a ubiquitous concept, central to cloud adoption and U.S. leadership. Enabling trust, as with all of the recommendations, is an incremental process and should not become a reason to resist moving to the cloud. The Commission recognizes that enabling trust is a pillar of cloud adoption and notes that recommendations in subsequent sections of this report also support enabling trust in the cloud.



In recent months, senior U.S. officials have described threats such as cyber crime and state-sponsored industrial espionage as outpacing many enterprise defenses. In this evolving cyber threat environment, the commission believes that cloud security services and solutions, if done correctly, may provide improved security relative to non-cloud environments.

Recommendation 1 (Security & Assurance Frameworks): Government and industry should support and participate in the development and implementation of international, standardized frameworks for securing, assessing, certifying and accrediting cloud solutions.

The Commission recommends that cloud-computing service providers collaborate with the National Institute of Standards and Technology (NIST), relevant associations and standards bodies to assess and evolve current best practices and standards, to strengthen cloud security metrics, and to facilitate information sharing.

Best Practices and Standards: Collaboration on best practices and standards should focus on identifying and addressing gaps in relevant domestic and international best practices and existing standards related to security, privacy, transparency, and accountability with respect to delivering trusted cloud computing services. The best practices and standards should be assessed in the context of the industry segments served by their respective provider types.[2]

In order to implement applicable best practices and standards around security and information assurance, the Commission supports the efforts underway on programs such as the Federal Risk and Authorization Management Program (FedRAMP) and NIST Security Content Automation Protocol (SCAP).

FedRAMP is a voluntary, General Services Administration (GSA) led initiative to develop and provide a standard approach to assessing and authorizing cloud computing services and products for use by Federal agencies. The Commission believes that a well-defined FedRAMP framework will help accelerate the adoption of cloud in the Federal government. The NIST SCAP is a standard that enables the automation of reporting and verifying IT security control parameters. SCAP provides a ready method to capture, test and continuously monitor the controls and integrity settings required to achieve the respective standard and/or compliance requirements.

Metrics: The Commission believes that cloud-related security metrics are critical for establishing a basis for trust in the cloud and recommends that industry collaborative efforts also address security measurement frameworks. Security measurement frameworks should include relevant security metrics that will allow potential customers to compare and select appropriate security levels for their cloud services. For example, a standard set of risk-based performance measures weighted and tailored for relevance to needs and matters of importance to each customer would enable potential customers to determine the appropriate security levels for their workload and data.

---

[2] Examples include the International Standards Organization (ISO 27001/27002), NIST (SP-800-53), and the Payment Card Industry Security Standards Council (PCI DSS)

Security metrics efforts should build upon industry and academia initiatives already chartered to address standard cloud performance measurement frameworks. Examples of such initiatives include the Carnegie Mellon University Cloud Services Measurement Initiative Consortium (CSMIC), the Distributed Management Task Force's (DMTF) Cloud Management Working Group, and the Cloud Security Alliance (CSA). This is also an opportunity to build on similar efforts of government agencies to develop standards, best practices, and key performance indicators (KPIs), such as in the work underway at NIST, the National Security Agency (NSA), GSA, and the Federal CIO Council.

To foster the development of measures and metrics, these collaborative efforts should also promote educational and research programs around cloud security. These types of frameworks and tailored criteria will allow public sector organizations to develop specifications pertinent to government and help formulate procurement guidance for cloud services.

By establishing and adopting standardized frameworks for securing, assessing, certifying, and accrediting cloud systems, cloud providers can deliver a higher level of transparency and trust to consumers. Transparency of real-time status and performance metrics associated with the confidentiality, integrity, and availability of cloud systems will further contribute to enhanced trust and confidence in secure cloud services.

Information Sharing: As the cloud is deployed by federal agencies and businesses in multiple sectors, cloud-related security issues will become an important element of the overall security discussion for those communities. The Commission therefore recommends that cloud expertise be integrated into existing information-sharing structures, such as the Information Sharing and Analysis Centers (ISACs) and the Sector Coordinating Councils.

Recommendation 2 (Identity Management): Industry and government should accelerate the development of a private sector-led identity management ecosystem as envisioned by the National Strategy for Trusted Identities in Cyberspace (NSTIC) to facilitate the adoption of strong authentication technologies and enable users to gain secure access to cloud services and websites.

Mechanisms to provide identity, authentication, and attribution in cyberspace are essential to accelerating adoption of cloud computing services and improving trust in the cloud. (For example, identity management facilitates access verification, billing, law enforcement access, and other features and capabilities.) Two characteristics of a robust identity management ecosystem are (1) enabling higher level transactions to occur electronically and (2) enabling credentials to be utilized across multiple services and websites. For the cloud, these have two benefits. First, a more robust authentication system would facilitate the transition of a wider variety of workloads and interactions to cloud services. Second, multi-use credentials would facilitate interoperability and allow customers to assemble the systems most appropriate for their workloads. In this case, a community of identity management systems will enable seamless transitions when data, processing tasks, and other applications reside on different

platforms at different service providers with different access control requirements, or when cloud services have to integrate with traditional IT systems.

The need for identity management capabilities is not new or unique to the cloud, and there is an opportunity to build on existing initiatives and innovation underway in this area. The National Strategy for Trusted Identities in Cyberspace (NSTIC, http://www.nstic.us/), released in April 2011, is aimed at developing a broad, private-sector led, identity management ecosystem that enables the identification and authentication of the individuals, organizations, and underlying infrastructure involved in an online transaction. The Commission endorses NSTIC's goal of facilitating creation and broad deployment of identity capabilities, and the adoption of cloud services by business and government will provide additional opportunities and motivation for development of this identity ecosystem.

In addition to supporting the development of a private sector-led identity management ecosystem, the Commission also suggests specific steps that the federal government could take as a user of cloud services that would contribute to advancing robust identity management:

- Deploy, as appropriate, multi-factor authentication for federal cloud applications as used by federal personnel and government contractors doing government contract work
- Accelerate the adoption of strong authentication, including multi-factor authentication and one time passwords, to enable mobile access to secure federal cloud services and websites

These actions are important because implementation of strong authentication will increase resilience of the cloud ecosystems. The Commission notes that the adoption of cloud technologies in the federal government continue in parallel with the coordinated development of these recommended systems rather than wait for a particular identity management solution.

The two preceding recommendations address some aspects of security and trust in the cloud; while security is certainly a critical element of trust in the cloud, it is not the only element. Good security is a continuous effort. This is true for all IT systems, not just the cloud.

A hypothetical target of perfect or near perfect security should not be used as an excuse for failing to use the cloud. Instead, the focus should be on whether the cloud provides security as good as or better than in-house IT deployments. The government should, of course, always seek to enable continuous improvement of security and the human and technical systems that connect to the cloud. This point is consistent with the discussions and recommendations throughout this report, such as those on monitoring, measuring, and information sharing; on risk assessment and management; on the importance of policies, people, and practices; and on research.

Recommendation 3 (Responses to Data Breaches): Government should enact a national data breach law to clarify breach notification responsibilities and commitments of companies to their customers, and also update and strengthen criminal laws against those who attack computer systems and networks, including cloud computing services.

Cloud services, like existing IT systems, will be the target of malicious actors. In addition to defending against attacks, the Commission notes that clarity around what should happen in the event of a data breach will serve both cloud consumers and providers. Timely notification and transparency to customers (individuals, organizations and governments) enables rapid response and the opportunity to minimize damage. Also, cloud service providers and law enforcement should have the tools needed to take action against criminal activity against clouds, such as breaching of data.

Specifically, the Commission recommends a national data breach law to streamline notifications and make it simple for customers to understand their rights with regard to notification. Such a law should include preemption of state laws to provide for harmonization. In addition, the law should take into account the various types of entities that are involved in processing the covered data cloud service providers, industry, government, nonprofit organizations, academic organizations, etc., and specifically provide that notice should be given by the entity that has a direct relationship with the parties whose information was subject to the breach. Finally, the law should have notification requirements based on risk of harm.

Note that the motivation for such legislation is not limited to cloud computing, but adoption of cloud computing would benefit from this action. Specifically, by clarifying responsibilities and commitments around notification, the law will enable cloud providers to prepare to take expected steps in case of a breach and enable customers to trust the providers to do so.

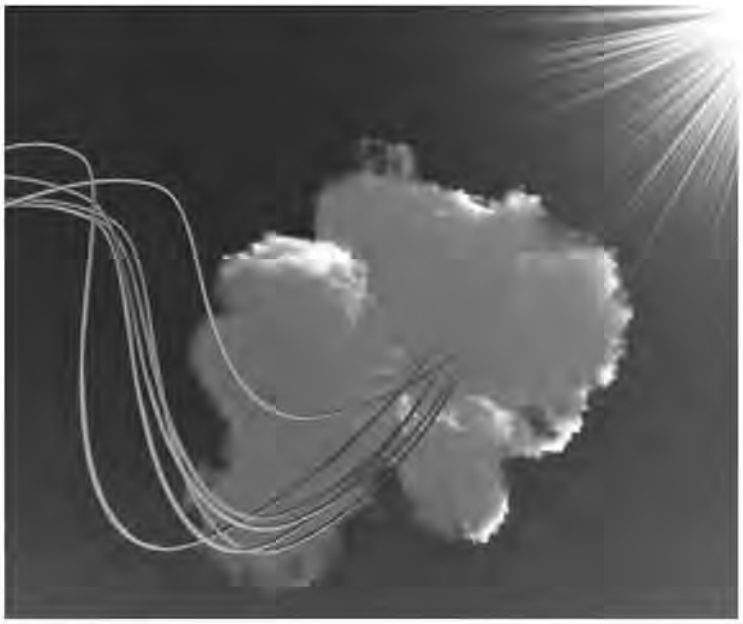
As a complement to the above recommendations, the U.S. government should update and strengthen criminal laws against those who attack our cyber infrastructure, including cloud computing services. In addition to clarifying cyber criminal offenses and defining penalties, the Federal government must commit adequate resources and personnel to investigating and tracking down cyber criminals. As much of cyber crime is transnational, the federal government should promote further international cooperation around cross-border prosecutions and identifying countries affording safe havens to such criminals.

Recommendation 4 (Research): Government, industry, and academia should develop and execute a joint cloud computing research agenda.

The Commission recommends that government, industry, and academia take responsibility for developing and carrying out a research agenda that will promote U.S. leadership in the cloud by enabling innovation that benefits customers and service providers. Relevant cloud-oriented research areas include, but are not limited to, usability, privacy, availability, integrity, confidentiality, security, cryptography, identity management, energy efficiency, resource allocation, portability, and dependability.

In conducting research on the cloud, industry should undertake short- and medium-term research where practical impacts are clear and investment risk is lower. Government research agencies, like the National Science Foundation (NSF) and the Defense Advanced Research Projects Agency (DARPA), should fund universities and other organizations to conduct long-range research activities, including those that build educational and research capacity and high-risk, high-reward projects. Cooperative cloud test beds will also be a critical element in advancing the overall evolution of cloud technologies.

Cloud technology has matured rapidly and will continue to develop. This recommendation should not be perceived as concern about cloud's current capabilities but rather as an investment in ensuring that the U.S. maintains a leadership role in the development, commercialization, and deployment of new cloud technologies and the expansion of cloud to new workloads, sectors, and activities. Basic research investments a decade ago yielded the ideas, technologies and capabilities that are fueling today's cloud developments. Continued innovation in the cloud will benefit directly from a sustained research agenda.



TRANSNATIONAL DATA FLOWS

The development and use of latest-generation information and communication technologies has allowed organizations and individuals to operate cloud-based services in any location around the world. The expansion of trade and business operations on a global level has also brought new challenges for operating in the global market. The globalization of business and trade through technology has resulted in multi-directional data flows and an exploding volume of data sources and stakeholders. This adds complexity to cloud adoption because of the data, process, and people residing on multiple continents with different laws and cultures. Despite these challenges, transferring data is an integral part of the cloud and must be addressed.



The recommendations classified within Transnational Data Flows address the need for collaboration across national borders and the need for international frameworks to standardize the processes. The Commission believes that recommendations to promote privacy frameworks, utilize performance-based criteria over proxy criteria that do not reflect specific and measurable attributes, and actions that overcome real and perceived challenges of transnational data flows are critical for the U.S. to adopt and lead in cloud computing. These actions are important because the United States must act as both a consumer of the cloud and as a leader in cloud innovation and markets. If the United States does not take a proactive position in both of these roles, the potential of a powerful global cloud market that enables individuals, industries and governments to innovate rapidly may not be fully realized.

Recommendation 5 (Privacy): The U.S. government and industry should promote a comprehensive, technology-neutral privacy framework, consistent with commonly accepted privacy and data protection principles-based frameworks such as the OECD principles and/or APEC privacy frameworks.

The Commission recommends that the U.S. build upon the work of existing, accepted privacy and data protection principles-based frameworks such as the Organization for Economic Cooperation and Development (OECD) and/or Asia-Pacific Economic Cooperation (APEC) to develop and promote a comprehensive, technology-neutral privacy framework. The existing U.S. laws are sector specific and state specific, and this approach is different than those in other regions (e.g., Europe). In some quarters, there is a concern that this may impede the transnational flow of data with other countries, especially those in Europe. These actions would help provide the certainty and flexibility required for continued cloud innovation and would be a step toward fostering a global market for cloud services. Industry should embrace such frameworks and utilize them to the fullest extent practicable.

Concepts of privacy are evolving in the Internet age, when information seldom has a single physical location, and duplication and sharing can occur quickly and easily. In addition, expectations around the norms and goals associated with privacy differ by culture, generation, and other factors. In this environment, the above recommendation is designed to demonstrate that the U.S. and U.S. companies take privacy seriously and to provide a basis for international discussions around mechanisms to resolve conflicting privacy policies. Such actions will also help overcome misunderstandings and confusion around the U.S. position on privacy; where uncertainty may be causing multinational and foreign organizations to avoid U.S.-based clouds or cloud computing altogether.

Recommendation 6 (Government/Law Enforcement Access to Data): The U.S. government should demonstrate leadership in identifying and implementing mechanisms for lawful access by law enforcement or government to data stored in the cloud.

The Commission recommends that the U.S. modernize legislation governing law enforcement access to digital information in light of advances in IT in general and the cloud in particular. Reform of the Electronic Communications Privacy Act (ECPA) is critical to clarifying the legal conditions under which U.S. cloud providers and their customers will operate, as technology changes have overtaken many aspects of ECPA as originally written. Various groups such as the Digital Due Process Coalition have proposed making government access to data stored in the cloud consistent with government access to data stored in in-house IT systems.

The U.S. Department of Commerce should conduct a study to assess the impact of the USA PATRIOT Act and similar national security laws in other countries on a company's ability to

deploy cloud in a global marketplace. This action may provide insights into how best to address the uncertainty and confusion caused by national security statutes (e.g., PATRIOT Act[3] and similar laws of other nations) that are perceived as impediments to a global market place for cloud services.

In addition, the U.S. government should take the lead on entering into active dialogues with other nations on processes for legitimate government access to data stored in the cloud and processes for resolving conflicting laws regarding data. These discussions should build on existing agreements and arrangements with other nations (e.g., expedited Mutual Legal Assistance Treaties and bilateral and multilateral agreements).

These three steps all will contribute to increasing clarity around the rules and processes cloud users and providers should follow in an international environment. Without U.S. leadership and cooperative international efforts, the world will face a far more complex legal environment, one that is not conducive to fully leveraging the cloud.

Recommendation 7 (E-Discovery and Forensics): Government and industry should enable effective practices for collecting information from the cloud to meet forensic or e-discovery needs in ways that fully support legal due process while minimizing impact on cloud provider operations.

Critical to improving trust in the cloud and accelerating adoption is the need for best practices in collecting forensic data and information in ways that do not result in significant, adverse impacts on individuals and/or organizations using the cloud-based information. To address this, the Commission recommends that the Federal CIO work with applicable agencies such as the U.S. Department of Justice and other relevant organizations to establish best practices specifically addressing acceptable methods for collecting forensic evidence from organizations using cloud-based information systems. In addition, cloud providers should assist their customers (e.g., individuals, commercial entities, government) with technologies to facilitate e-discovery and information retrieval requirements, whether in support of regulatory compliance or litigation activities.

Specific issues that will need to be addressed include methods to facilitate cooperation among service providers, how best to maintain a verifiable chain of custody, how best to collect data from proprietary technologies, and how best to minimize service availability impacts resulting from seizures of data and equipment. Improving the processes and practices around evidence collection and forensics will improve cloud customers' confidence in continuity of service and

[3] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001

their ability to meet legal requirements. It will also provide tools to support the tracking and prosecution of cybercriminals (as discussed in Trust Recommendation 3).

Recommendation 8 (Lead by Example): The U.S. government should demonstrate its willingness to trust cloud computing environments in other countries for appropriate government workloads.

This recommendation highlights the role of the U.S. government both as a customer of cloud services and as a leader in enabling trustworthy use of the cloud.

Government agencies, in evaluating potential models for using the cloud, should not assume or default to the notion that no government workload and/or task is suitable for cloud computing environments in other countries. Instead, they should carefully consider the types of data and tasks within their information and communications technology portfolios to match suitable workloads to the cloud computing models that achieve the required level of confidentiality, integrity, and availability at the appropriate levels of efficiency, cost, and redundancy. Evaluation of the specific workload and/or task needs is necessary to determine suitable potential cloud computing environments and models.

By evaluating cloud services based on the performance needs of specific workloads, the U.S. government can show leadership in the adoption of approaches that recognize the multiple factors that contribute to ensuring trust in the cloud (see discussion around Trust Recommendation 1). The development of the frameworks, best practices, metrics, and standards to enable this approach should help businesses and other governments take a similarly comprehensive approach to trusted cloud deployment.

While the Commission is not declaring that no circumstances exist in which certain types of federal data could be limited to U.S. storage, it is critical to understand that location is but one factor in the security of information, and location should not be viewed as a proxy for security in the cloud. For example, effective use of security technologies, including technologies to make data unreadable and unusable, is as important, if not more important, than location in enhancing the security of data in the cloud.

Cloud providers typically locate data centers based on a variety of factors, including technical issues like network topology, economic issues like the price of electricity, and business issues like proximity to markets. Once data centers have been built, however, the storage and processing of data can occur in multiple data centers and across geographic boundaries and legal jurisdictions. For some customers and workloads, the preference might be to allocate storage and processing locations based on technical and economic factors (perhaps to maximize speed, or minimize cost). For other customers and workloads, there may be concerns about data touching certain legal jurisdictions that impose data handling requirements around privacy, retention or other legal or regulatory burdens.

To service customers with such concerns, cloud providers could enable the setting of policies around specific data and workloads to control what legal jurisdictions those data or workloads may enter and enable tags to carry provenance attesting to those locations. (The discussion above about the need to conduct international dialogues on methods for resolving inconsistent rules between countries is also a critical step toward dealing with these concerns.)

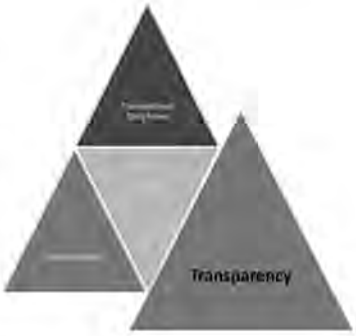
The Commission encourages adoption of approaches that give cloud providers the flexibility to develop and deploy services for a diversity of workloads in innovative ways, rather than constrain cloud services by geography. This will allow users, when appropriate, to take advantage of the potential benefits in access, reliability, resiliency, efficiency, and costs that can result from geographical distribution of workloads.



TRANSPARENCY

U.S. leadership in the cloud will be facilitated if cloud providers make a firm commitment to transparency. Transparency in the context of cloud computing requires vendors to share relevant information about their capabilities, offerings, and service levels.

Transparency by cloud vendors will encourage the shift to the cloud by addressing some of the primary reasons federal agencies and commercial companies do not move to the cloud: uncertainty about how systems outside of their control will perform and fear of being unable to access or move their data. We offer two recommendations specifically designed to allay these concerns by ensuring customers maintain control over the performance of their systems and access to their data while still realizing the cost, efficiency, and scalability advantages of cloud computing.



Recommendation 9 (Transparency): Industry should publicly disclose information about relevant operational aspects of their cloud services, including portability, interoperability, security, certifications, performance and reliability. Industry and government should support development of metrics designed to meet the needs of different user groups. These metrics should be developed in an open and transparent environment, taking into account the global nature of cloud use.

The Commission recognizes the need for information and tools that provide users with meaningful ways to evaluate the characteristics and performance of various cloud implementations, whether they are contemplating deployment or evaluating performance of their current services. Development of metrics around key cloud attributes should be driven by user needs and provider capabilities. The government and commercial sector should collaborate on lessons learned, and each should be careful to avoid dominating the development of these metrics. Different government and business sectors will likely demand different measures and tools.

Currently, the lack of transparency and standard metrics make it difficult for customers to compare the cloud offerings of different providers. Unsure about what they are being offered and unclear on the differences among the cloud options available, many customers hesitate before moving to the cloud or decide to delay moving to the cloud until there is agreement on common metrics that facilitate easy comparison of cloud providers. The Commission encourages industry to work with the appropriate government agencies to create customer tools that make "apples-to-apples" comparisons possible among different cloud providers and the services that they provide. This will increase the confidence commercial and government customers have in moving to the cloud and will accelerate cloud adoption.

Recommendation 10 (Data Portability): Cloud providers should enable portability of user data through documents, tools, and support for agreed-upon industry standards and best practices.

One benefit of the cloud is its ability to store and process large quantities of data. For customers making the transition to cloud, this often raises questions about how they access or move that data, especially in cases where they are switching between cloud providers. Data portability can be achieved in a variety of ways, and cloud providers should be transparent about their conformance with industry standards and best practices as well as the documents, tools, and relevant third-party solutions they make available to their customers. Customers should recognize that early consideration of data portability in selecting and implementing cloud services can reduce the risk of vendor lock-in.

A collection of data portability standards, formats, and practices is vital to encouraging widespread cloud adoption. Government and industry should collaborate on facilitating the rapid development and dissemination of these standards and other relevant tools. The collaboration between NIST and the private sector in preparing the NIST standards roadmap under the Federal Cloud Computing Strategy is an excellent example of these types of efforts.

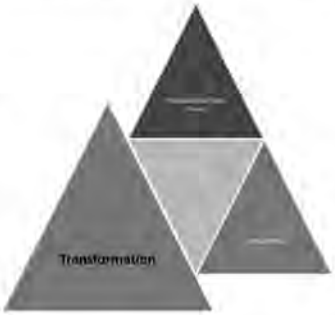
This work should serve as a model for future efforts around data portability and could be extended to other facets of cloud including workload and application portability. Both government and industry should continue to emphasize open, multi-vendor, unencumbered standards and best practices.



TRANSFORMATION

Cloud computing is a disruptive technology that has significantly changed the IT landscape. Although cloud computing offers many benefits to adopters, it also poses challenges to Federal agencies and commercial organizations that are trying to adapt to the technological changes ushered in by the cloud. To achieve the benefits offered by cloud computing, government and industry need to be open to re-envisioning the role of IT and willing to make the investments necessary to harness the power of the cloud.

The first two recommendations in this section focus specifically on actions that the federal government can take to facilitate the transition to cloud. By stepping forward as a leader in the adoption of cloud computing, the federal government can play a key role in driving innovation and economic growth in the IT industry and demonstrate that it considers the cloud an important, effective, safe and secure environment. The second two recommendations focus on the transformation in infrastructure and workforce that are necessary for widespread cloud adoption.



Recommendation 11 (Federal Acquisition and Budgeting): Agencies should demonstrate flexibility in adapting procurement models to acquire cloud services and solutions. Congress and OMB should demonstrate flexibility in changing budget models to help agencies acquire cloud services and solutions.

In interviews with senior government officials, the Commission found that the current Federal Acquisition Regulation (FAR) does not need alteration for agencies to acquire cloud services. The FAR is already flexible enough to allow agencies to acquire IT as a service. However, agencies should demonstrate flexibility in adapting current procurement models and existing contracts to take advantage of new cloud offerings.

Table 1: Top Priorities for Spending

Priority	Ranking
Lowering costs	1
Integrating systems and processes	1
Implementing security and privacy measures	1
Project management improvements	4
Staff development/retention/ recruiting	5
Transparency and performance management initiatives	5
Stimulus support	7

Source: Federal CIO Survey, TechAmerica (May 2011)

One of the biggest challenges agencies may face in budgeting is predicting the costs of cloud computing over the course of a fiscal year. Cloud computing is designed to scale quickly to a customer's needs, providing maximum flexibility to the user. If the cloud service is based on a predictable subscription model (such as a standard monthly fee per user), these budget projections can be easily accommodated. If the cloud service is based on pay-as-you-go usage, however, it can be difficult to predict costs unless the user can precisely forecast future computing needs. To address this challenge, the Commission recommends that the current efforts to update and streamline the OMB 300 exhibit form and associated budget scoring include tools that facilitate and encourage the new business models associated with cloud. OMB and Congress should communicate to agencies that it recognizes budgeting for cloud is not like budgeting for traditional IT services and should assure agencies it will provide support and flexibility during and after the transition to the cloud.

To help agencies acquire cloud services, the Commission also recommends Congress and OMB demonstrate flexibility in changing budget models. Agencies currently face challenges transitioning funds between capital expenditure (also known as acquisition) accounts and operations and maintenance expenditure accounts when adopting and implementing cloud services and solutions. Most in-house information systems rely upon funding from capital expenditure accounts, while cloud services and solutions do not have intensive capital expenditures and are funded more from the operations and maintenance expenditure accounts.

Agencies today, however, are hampered and even prevented from transitioning funds from the capital expenditure accounts to the operations and maintenance expenditure accounts, even

when there are overall savings to be realized by the shift in IT approaches that requires the transition of the funds. This creates a disincentive for agencies to really drive savings and efficiencies through adoption of cloud services and solutions. Government must find ways to provide more flexibility for agencies to reduce and transition funds in the capital expenditure accounts to the operations and maintenance expenditure accounts as part of implementing innovative cloud solutions and achieving savings.

In making decisions about budgeting and acquisition, federal agencies, through the CIO Council, would benefit from sharing best practices, tools for objective analysis of cloud performance, and ways to predict and document different contributors to the budgetary impact of switching to the cloud. To ensure that the CIO Council can provide this support to federal agencies, it should include experts from a wide array of communities, including chief financial officers, chief acquisition officers, human capital officers, and program managers. Additionally, staffing OMB's other councils, such as the CAO and CFO Council, with cloud expertise could ensure these councils can also provide support to agencies implementing cloud.

As agencies are creating their business cases and preparing to move to the cloud, it is important to remember that the adoption of cloud is a multi-stage process. Initial deployments by government may not take full advantage of the potential capabilities and benefits of the cloud, but these steps are necessary for customers to explore new (and sometimes fundamentally different) approaches to selecting, acquiring, and utilizing IT. When agencies are in a transition to the cloud, it is critical that they take care that the policies and standards of the cloud provider do not lock the agency into an early deployment model. Agencies should require that policies be flexible enough to allow evolution of use and innovation through the adoption of new infrastructure, services, and applications.

Recommendation 12 (Incentives): Government should establish policies and processes for providing fiscal incentives, rewards and support for agencies as they take steps towards implementing cloud deployments.

Adopting a new technology can be difficult, and the transition of agencies to the cloud will require investment of time, resources, and political will by the federal government. In recognition of this, the Commission recommends that OMB establish incentives and provide support for agencies beginning cloud adoption.

On the fiscal side, agencies may be hesitant to undertake a significant change to their IT structure during a time of budgetary constraint or may have difficulty finding and justifying the costs associated with an IT transition. One possible incentive is to allow agencies to retain and redirect a portion of

Table 2: Reported cloud computing activities, 2009 and 2011

Cloud related activity	Late 2009	Early 2011
Active project to move to cloud computing	54%	57%
Undertaking cloud pilot	16%	14%
Tracking OMB/ awaiting direction	22%	21%
No current plans for cloud	8%	0%
Other	0%	7%

Source: Federal CIO Survey, TechAmerica (May 2011)

the overall budget savings realized from cloud adoption. Another approach is to provide seed money to agencies that help with the initial investments required in moving to the cloud.

OMB could also support agencies in the cloud transition by providing assistance in the processes that govern the transition. OMB and GSA assistance on moving from static to more dynamic assessment and authorization processes, change management, and compliance with OMB guidance would help facilitate the transition.

In addition to financial support and process assistance, public recognition and praise for agencies that are early adopters of cloud computing or deploy the cloud in particularly innovative ways is important. Individuals within agencies who have played key roles in enabling a cloud transition should also be recognized with service or financial awards. This sort of public support should be complemented by public acknowledgement by agency and Administration leadership that there are risks inherent in adopting a new technology infrastructure; this would provide some support for agency staff during the process of implementing the cloud transition.

Recommendation 13 (Improve Infrastructure): Government and industry should embrace the modernization of broadband infrastructure and the current move to IPv6 to improve the bandwidth and reliable connectivity necessary for the growth of cloud services.

The Commission recommends that the federal government and industry continue to expand deployment of high bandwidth networking, enhance network resilience, and advance IPv6 adoption to ensure ample broadband connections.

The Commission recommends government and industry initiatives designed to increase the deployment and adoption of both wired and wireless broadband, especially to underserved areas of the country. Efforts such as those advocated in the Federal Communications Commission's National Broadband Plan, including making additional spectrum available and expanding opportunities for opportunistic and unlicensed spectrum use, are necessary to allow cloud computing to function effectively and for businesses and citizens to realize the benefits of innovative new cloud technologies.

With rapidly rising demands for connectivity, the last batch of IPv4 addresses, assigned earlier this year, is unlikely to meet demand beyond the end of 2011. Since cloud computing depends on the connection of many individuals, devices, and locations, a quick transition to IPv6 is vital to ensuring the successful adoption and operation of cloud computing in the future. The Commission applauds the government's move to enable the use of IPv6 on external servers by October 2012 and on internal networks by 2014.

Recommendation 14 (Education/Training): Government, industry, and academia should develop and disseminate resources for major stakeholder communities to be educated on the technical, business, and policy issues around acquisition, deployment and operation of cloud services.

The transition to the cloud will require new capabilities for a variety of communities. The business community (and agency leaders) will need to understand how cloud changes the economics of their IT expenses and provides new capabilities through which to carry out their lines of business (or agency missions). Acquisition workforces will need new skills to gather and assess the information necessary to make informed purchasing choices. The responsibilities of IT workforces will expand to manage new cloud capabilities and, within cloud customers, the IT expertise needed will evolve as activities such as operations, maintenance, and development are shared or shifted to cloud providers.

Acquisition Workforce: The Commission commends GSA's outreach efforts to federal agencies to provide materials, expertise, and support around investigating, procuring, and deploying cloud solutions. GSA could build on this work by creating a cloud educational portal to help agency buyers, architects, administrators, and end users in understanding all aspects of cloud computing. Resources for this portal might include white papers, articles, and training materials.

IT Workforce: Government, using existing programs in technology education and workforce training,[4] can facilitate and encourage academic institutions and educational organizations to develop and offer courses relevant to cloud, in partnership with industry. Industry and academia can help develop curriculum relevant to new technologies and skills (in partnership with the educational institutions and organizations), and support employee retraining.

Workforce education should embrace a spectrum from informal outreach to disseminate introductory or reference materials to targeted courses in specific skills and areas to integration of cloud-related topics into overall curricula in formal programs in computer science and engineering, project management, business schools, and other relevant areas. On the informal side, outreach to IT professionals could disseminate information about cloud issues, skills, and opportunities. Within the government, outreach and support networks for acquisition personnel would provide an opportunity to share experiences and best practices.

---

[4] The Department of Labor, the Department of Education, and the National Science Foundation all have programs in technology education and workforce training that might support activities relevant to cloud computing.

Conclusion

In a time when the government is seeking to do more with less and the commercial sector is being called upon to create jobs and grow the economy, now is the time to act on the cloud. Cloud computing has ushered in vast improvements in the cost, agility and efficiency of computing. These benefits alone drive a strong business case; however, the more compelling return is the opportunity to leap forward; to discover new markets and improve how we interact with, serve, and support U.S. citizens, users and other nations. The cloud holds the potential to unlock widespread entrepreneurism of all shapes and sizes, and expand the scope to do entirely new things — innovations such as social networking, which we could not fully imagine just a decade ago, would not exist without IT's continued evolution to the cloud.

Despite the clear benefits of cloud computing, many challenges impede its widespread adoption. These challenges face both those ready to embrace the cloud and those grappling with doubts about making the move. Those who are ready address challenges such as training acquisition personnel and determining which workloads should be moved to the cloud; those who are hesitant have concerns about, for example, the security of and control over data stored and workloads processed in the cloud. If unaddressed, these challenges threaten to slow the acceptance of cloud computing and delay the enormous advantages and opportunities it provides. To address the challenges and allay concerns, the Commission has offered in this report a range of practicable recommendations; these show the way forward to those ready to adopt the cloud, and guide cloud providers and users in addressing the issues of those not yet prepared to shift.

The Commission recognizes that industry and government share responsibility for enabling cloud's adoption and for leading in the cloud evolution. Reflecting the urgency to provide incremental movement, create momentum and lead through actions, many of the recommendations target short-term tactical and operational advances. Complementing these are longer term recommendations that reflect the strategic importance of the evolution, and the mandate to look beyond the cloud we know today, to the opportunities it creates for the future.

It is the hope of this Commission that the federal government, industry and academia will implement these recommendations and be leaders in shaping how the future unfolds through the adoption of the cloud across the United States and around the world. Furthermore, these recommendations should demonstrate that cloud computing is not a new technology that needs further validation or analysis before it can be safely adopted; it is a natural evolution in computing. Those who recognize this and take early advantage of the benefits it offers will, in the coming decades, be the leaders not in only IT but in driving the cloud's evolution, and therefore, in driving business and mission results.

Recommendations

Recommendation	Industry	Government	Academia	Short-Term	Long-Term
Recommendation 1 (Security & Assurance Frameworks): Government and industry should support and participate in the development and implementation of international, standardized frameworks for securing, assessing, certifying and accrediting cloud solutions.	•	•			•
Recommendation 2 (Identity Management): Industry and government should accelerate the development of a private sector-led identity management ecosystem as envisioned by the National Strategy for Trusted Identities in Cyberspace (NSTIC) to facilitate the adoption of strong authentication technologies and enable users to gain secure access to cloud services and websites.	•	•		•	
Recommendation 3 (Responses to Data Breaches): Government should enact a national data breach law to clarify breach notification responsibilities and commitments of companies to their customers, and also update and strengthen criminal laws against those who attack computer systems and networks, including cloud computing services.		•		•	
Recommendation 4 (Research): Government, industry, and academia should develop and execute a joint cloud computing research agenda.	•	•	•		•
Recommendation 5 (Privacy): The U.S. government and industry should promote a comprehensive, technology-neutral privacy framework, consistent with commonly accepted privacy and data protection principles-based frameworks such as the OECD principles and/or APEC privacy frameworks.		•			•

Recommendation	Industry	Government	Academia	Short-Term	Long-Term
Recommendation 6 (Government/Law Enforcement Access to Data): The U.S. government should demonstrate leadership in identifying and implementing mechanisms for lawful access by law enforcement or government to data stored in the cloud.		•		•	
Recommendation 7 (E-Discovery and Forensics): Government and industry should enable effective practices for collecting information from the cloud to meet forensic or e-discovery needs in ways that fully support legal due process while minimizing impact on cloud provider operations.	•	•		•	
Recommendation 8 (Lead by Example): The U.S. government should demonstrate its willingness to trust cloud computing environments in other countries for appropriate government workloads.		•			•
Recommendation 9 (Transparency): Industry should publicly disclose information about relevant operational aspects of their cloud services, including portability, interoperability, security, certifications, performance and reliability. Industry and government should support development of metrics designed to meet the needs of different user groups. These metrics should be developed in an open and transparent environment, taking into account the global nature of cloud use.	•	•		•	
Recommendation 10 (Data Portability): Cloud providers should enable portability of user data through documents, tools, and support for agreed-upon industry standards and best practices.	•			•	

Recommendation	Industry	Government	Academia	Short-Term	Long-Term
Recommendation 11 (Federal Acquisition and Budgeting): Agencies should demonstrate flexibility in adapting procurement models to acquire cloud services and solutions. Congress and OMB should demonstrate flexibility in changing budget models to help agencies acquire cloud services and solutions.		•		•	
Recommendation 12 (Incentives): Government should establish policies and processes for providing fiscal incentives, rewards and support for agencies as they take steps towards implementing cloud deployments.		•			•
Recommendation 13 (Improve Infrastructure): Government and industry should embrace the modernization of broadband infrastructure and the current move to IPv6 to improve the bandwidth and reliable connectivity necessary for the growth of cloud services.	•	•		•	
Recommendation 14 (Education/Training): Government, industry, and academia should develop and disseminate resources for major stakeholder communities to be educated on the technical, business, and policy issues around acquisition, deployment and operation of cloud services.	•	•	•	•	

Acknowledgements

TechAmerica Foundation gratefully acknowledges the contributions of the Commissioners, their colleagues and staff to the successful completion of this report on the Leadership Opportunity in U.S. Deployment of the Cloud (CLOUD^2). Moreover, the Commission interviewed and collected input and feedback from people with academic, government and industry backgrounds. We express our thanks for their participation in this effort and the valuable knowledge and innumerable years of experience they shared to inform the recommendations of this report.

Robert Brese, Department of Energy
Greg Buckles, eDiscovery Journal
Steven Chabinsky, Federal Bureau of Investigation
Kathy Conrad, General Services Administration
Jim Dempsey, Center for Democracy and Technology
Patrick Gallagher, National Institute of Standards and Technology
Bob Gourley, Crucial Point LLC
Damon Greer, International Trade Administration
Vivek Kundra, Office of Management & Budget
Dawn Leaf, National Institute of Standards and Technology
Mary Lewin, General Services Administration
Gary Locke, Department of Commerce
Dave McClure, General Services Administration
Bajinder Paul, General Services Administration
Lisa Schlosser, Office of Management and Budget
Ari Schwartz, National Institute of Standards and Technology
Adam Sedgewick, General Services Administration
Dennis Smiley, Department of Homeland Security
Richard Spires, Department of Homeland Security
Larry Sweet, National Aeronautics and Space Administration
Teri Takai, Department of Defense
Keith Trippie, Department of Homeland Security
Peter Tseronis, Department of Energy
Phillip Verveer, Department of State
Neal Ziring, National Security Agency

Commission on the Leadership Opportunity in U.S. Deployment of the Cloud (CLOUD^2)

Deputy Commissioners

Amy Alving
SAIC

Jerry Archer
Cloud Security Alliance

Veena Avula
Informatica Corporation

Gregg "Skip" Bailey
Deloitte LLP

Heather Blersch
General Dynamics Information Technology

Peter Bogdonoff
AgilePath Corporation

Mark Bohannon
Red Hat, Inc

Bob Bonham
SAS

Emerson Brooks
SRA International

Paul Brubaker
Syntractive

Dan Burton
Salesforce.com

Pam Carpenter
Adobe

Nick Combs
EMC Corporation

Michael Donovan
HP Enterprise Services

David Dudas
Sorenson Media, Inc.

Carolyn Eichler
CSC

Danielle Estrada
Accenture

Steve Estrada
OpenConnect

Sarah Falvey
Google, Inc.

Andrew Gastwirth
Attain, LLC

Eric Green
CSC

Melvin Greer
Lockheed Martin IS&GS

Justin Greis
Ernst & Young

Elizabeth Grossman
Microsoft

Dan Guerra
International Computerware, Inc.

Randy Hahn
Verizon Business

Phil Harris
VCE

Mel Hurley
Wyle Information Systems

Kirk Kern
NetApp

Christie Kestler
Savvis

Mandeep Khera
Cenzic, Inc.

Jeff Koch
IBM Corporation

David Laliberté
Research In Motion, Limited

Jeff Lawton
Grant Thornton

Curtis Levinson
Qwest Government Services, Inc.

Marc Lucas
GCE

Chris Mankle
ACS, A Xerox Company

Ben Marglin
Booz Allen Hamilton

Atul Mathur
IMC, Inc.

Steve McCummings
Cisco Systems Inc.

PG Menon
Brocade Communications Inc

Nick Mistry
eGlobalTech

James Morin
Ciena Corporation

Sergio "Checo" Muniz
MEI Technologies, Inc.

Vishy Narayan
Infosys

Thomson Nguy
Amazon, AWS

Jim O'Hara
LiveOffice

Tom Parker
Securicon

Kevin Paschuck
RightNow Technologies

William Perlowitz
URS-Apptis

Brendan Peter
CA Technologies

Arnie Phatak
Syntel

John Pientka
CGI Federal

Chris Poelker
FalconStor Software

Braden Preston
Harris Corporation

Margaret Rooney-McMillen
AT&T Business Solutions

Jim Rottsolk
Microsoft

Glenn Schoonover
Qualys

Duke Skarda
SoftLayer Technologies

David Smith
Citrix

Kirk Smith
L-3 Communications

Monica Smith
Teradata Corporation

Melissa Smolensky
Rackspace Hosting, Inc.

Emily Stampiglia
VCE

Jim Sweeney
GTSI Corp

Franco Tao
Information Innovators, Inc.

Scott Turicchi
J2 Global Communications, Inc.

Leif Ulstrup
CSC

Jacqueline Vanacek
SAP AG

Herb VanHook
BMC Software

David Vennergrund
Delta Solutions and Technologies, Inc.

Bob Wambach
VCE

Bryan Ward
Serco North America

Steven Warner
Northrop Grumman Corporation

CLOUD^2 Staff

D. Zachary Champ
TechAmerica Foundation

Randi Meyers
TechAmerica Foundation

Launched in 1981, TechAmerica Foundation is a 501(c)(3) non-profit affiliate of TechAmerica. It disseminates award-winning industry, policy, and market research covering topics such as U.S. competitiveness in a global economy, innovation in government, government IT forecasts, technology employment and international trade indicators, and other areas of national interest.

TechAmerica
FOUNDATION

601 Pennsylvania Avenue, NW
North Building, Suite 600
Washington, DC 20004
202.682.9110 (T)
202.682.9111 (F)
TechAmericaFoundation.org

Prepared Statement of William Weber, General Counsel, Cbeyond, Inc.

Mr. Chairman and members of the Subcommittee, Cbeyond appreciates the opportunity to provide a statement for the record for today's hearing. Cbeyond provides cloud and communications services to more than 62,000 small and medium businesses (SMBs) nationwide; in our most established markets including Atlanta, Dallas, Denver and Houston, we provide services to more than 15% of all businesses with between 5 and 250 employees. Our annual revenue is nearly $500 million, and we have approximately 2000 employees. Forbes magazine recently named us one of America's Most Trusted Companies and—together with Kraft Foods and Timberland—we were recently given the Points of Light Corporate Engagement Award of Excellence.

I hope today to give you a brief overview of what cloud computing is, why it matters to SMBs, the role that competitive telecommunications providers play in advancing the technology and barriers that may prevent SMBs from making use of the cloud to create jobs and drive innovation.

What Is Cloud Computing?

Unfortunately, I am old enough to remember the giant computers of the 1960's with their punch cards and putty-colored terminals with ghostly green type. These machines differed from the computers our children grew up with in that their computing power was not in the terminals themselves; the computing power was in a mainframe computer located in another room or another building. This was why you sometimes heard the machines you typed on described as "dumb terminals."

Beginning in the late 70's and moving through the 80's, computing power gradually migrated from the network core to the network edge. This was the rise of the personal computer, and as competition blossomed and prices tumbled, true computing power became available to home and small business users for the first time. This democratization of computing resources remade our economy and fundamentally changed the way many of us work.

As PCs became ever smarter, faster and cheaper, we began to make demands on them that were difficult to achieve without a network. So we built a new kind of network. These new networks were fundamentally different from the old because now the computing power resided primarily at the edges. The networks themselves served to route information (like email) from PC to PC and to store information in central locations that needed to be accessed by many people simultaneously (like databases).

Soon, though, we discovered a need to return some real computing power to the network itself. Let's take a law firm as an example. By the mid-90s, law firms got tired of having to buy the same programs for all their computers, particularly the programs they used to bill their time, store and access important documents and organize their calendars. Software makers responded by creating versions of their software that could reside on a central server connected to individual computers via the Ethernet cables of the law firm network. Now multiple attorneys and assistants could access the same central information, bills could be generated automatically and the vast document databases that made legal work simpler could be shared, searched and accessed by dozens of people simultaneously.

This model worked well, but it had one major drawback: it required the law firm to maintain what amounted to a server farm on their premises and extensive Information Technology (IT) staff to take care of the servers and the internal network. It was also capital intensive because the firm had to purchase enough servers to run their enterprise software applications and back all those applications up. And, of course, they had to buy more resources than they actually needed to account for potential growth and be able to respond immediately to problems with an individual server; for a law firm—as with any other business—downtime would mean lost revenue. And this brings us to what people call "the cloud."

So what is the cloud? At a high level it is the movement of server-based computing power off the premises and onto servers that users access in a remote location over a private network or, in many instances, over the Internet. You already know about more consumer-focused, cloud-based services than you may think. Netflix's streaming video service is one. Facebook is another. Both these applications store vast amounts of information on remote servers somewhere on the Internet and deliver that information (and the computing power necessary to process it) to you on demand.

Why Do SMBs Care About the Cloud?

Understanding the basics of cloud computing is important, but it is just as important to understand how the businesses in your home districts use the cloud. A few examples might look like this:

- A seventeen-location Los Angeles furniture company sending all of its security footage directly to the cloud where they can store it securely and use server processing power to review and search it.
- A major insurance company with its US headquarters in Minnetonka moving its IT test environment to Amazon servers to avoid the capital costs associated with purchasing dozens of servers it will only need several times a year.
- A mid-size law firm with offices in Atlanta, Charlotte and Louisville moving its billing, time-keeping and accounting software to Cbeyond servers so that all of its offices can access the same data at the same time.
- A group of orthopedic surgeons in Denver moving all its patient records to the cloud to avoid the cost of maintaining the servers necessary to store, search and access x-rays and to ensure it meets its HIPPA obligations.

Why would these businesses want to move these applications and information to off-premise servers? There are many reasons, some of which are embedded in the examples above. First, getting someone else to manage their servers allows an SMB to focus on their business rather than their infrastructure. Lawyers want to practice law, doctors want to practice medicine, real estate agents want to close deals and architects want to design buildings. They don't want to spend time taking care of internal IT resources. Cloud computing allows them to realize this dream.

Second, cloud computing allows companies to preserve capital. Rather than buying servers that they then have to pay to maintain and upgrade, the business can rent only the server capacity it needs for the time it needs it. There are no installation cycles and no need for extra square footage or additional air conditioning or electrical upgrades.

Third, cloud computing is fundamentally more secure in a variety of ways. It is physically more secure because data centers—unlike most places of business—are consciously designed to the highest access security and fire control standards. Business data is also more secure because a server operating in a data center is monitored around the clock and potential failures can often be detected and dealt with before they occur; this kind of monitoring and response simply cannot occur in SMB IT environments. Data in the cloud can be backed up to multiple, geographically diverse locations automatically; if there is a tornado that destroys a data center in Indianapolis, a business can seamlessly and without pause access that data from its duplicate in a Denver data center. And, finally, servers in a data center are sitting behind the most sophisticated, well-monitored firewalls available, and their anti-virus software is constantly updated with no intervention or action required by the business; it's all part of the service a business buys when it moves its data to the cloud.

Fourth, cloud computing gives a business IT flexibility in that they can grow and shrink their computing resources on-demand, preserving both capital and time. If a business needs to test major software releases under heavy loads a few times a year, it can simply spin up cloud servers, run their tests and then spin them down, saving time, saving money and avoiding the cost of infrastructure it has only occasional need for.

Finally, the cloud allows businesses to increase IT velocity. If an innovator has an idea, it can be put to the test immediately. No more waiting for a server to ship and get installed. This compresses planning cycles, keeps our entrepreneurs focused on innovation rather than the infrastructure of innovation and allows new ideas to launch at the speed of the idea rather than the speed of FedEx.

How Do Competitive Telecommunications Providers Help SMBs Take Advantage of Cloud Computing?

If my comments thus far make cloud computing sound like the answer to many of the problems that SMBs confront as they launch or grow, good. Because that's an accurate view: cloud computing helps preserve capital, increases security and makes launching or growing a business both cheaper and faster. But SMBs need help to make the best use of cloud computing, help that can only come from their service providers.

Unlike the large businesses that first began making use of the cloud, SMBs do not have extensive IT resources. They don't know how to move the applications that

run their business into the cloud, and they don't know how to migrate the associated data. In fact, they generally don't even know what cloud computing resources they actually need to do whatever it is they want to do.

The large telecommunications and large cloud-only providers do a great job serving enterprise businesses with big IT staffs who know exactly what they need. The giant telecom companies and cable providers also provide high-quality services to the small businesses that need basic services like Internet bandwidth, phones and email. But what about the sophisticated SMB that wants to use the cloud to preserve capital for job creation and innovation? They are in a tough spot: they don't have the IT staff to help them with their migration to the cloud, and the big cloud providers are not set up to help them get QuickBooks and similar enterprise applications up and running in their data center. This is where companies like Cbeyond can help.

Competitive telecommunications providers are the experts in the technology needs of SMBs because it's all we do. We have direct sales people who introduce businesses to the power of the cloud and personnel whose only job is to help businesses choose exactly the resources they need for the job at hand. We innovate to serve our small business customers by creating cloud offerings tailored specifically to their needs, building applications specifically designed to migrate their data and providing the kind of personalized support they need to succeed. In short, without competitive telecommunications providers, most SMBs will simply be shut out of the cloud computing revolution to the detriment of our economy, our unemployment rate and our global competitiveness.

What Are the Barriers that May Prevent SMBs from Making Use of the Cloud to Create Jobs and Drive Innovation?

As the Committee well knows, small business is the economic engine that drives our economy and creates more jobs than any other sector. Small businesses inject almost a trillion dollars into the economy each year. They have created more than ninety-three percent of all new jobs over the last twenty years and employ more than half of the U.S. workforce. They also employ forty-one percent of the nation's high-tech workers who generate about thirteen times more patents per employee than do workers at large firms. SMBs that want to leverage the cloud to launch, grow, innovate and create jobs face two primary obstacles: assistance with their migration—which I discussed above—and abundant, high-quality bandwidth.

Cloud services are broadband intensive. Unlike traditional web-based services in which the heaviest bandwidth usage is downstream-only, an SMB using QuickBooks or other applications in the cloud is sending and receiving large volumes of data in both directions; it needs at least 10 megabits per second of private, symmetrical Ethernet bandwidth. While this may not sound like a lot in an age when cable companies routinely dangle 100 Mbps claims in the market, the key adjectives here are "private" and "symmetrical." What this means in plain language is that an SMB accessing cloud-based enterprise applications needs bandwidth that is not shared and has a guaranteed upstream speed that is the same as its guaranteed downstream speed.

Unfortunately, competitive technology providers—the real innovators in the cloud for SMBs—are limited by aging rules administered by the Federal Communication Commission (FCC) that have the perverse effect of locking small businesses into the broadband status quo of six years ago, undercutting the normal business cycle of innovation and denying our nation's SMBs benefits they should have received as broadband technology improved. These rules force competitive technology providers to buy the wholesale broadband inputs they need to reach their customers in small, 1.5 Mbps increments of time-division multiplexed (TDM) bandwidth; TDM technology was invented in the 1870s for the telegraph and evolved to its current form in 1962. This broadband gap leaves the rollout of the best cloud technologies almost exclusively to in the hands of large enterprise customers while innovative technology competitors try to serve SMBs, the job growth engine of our economy, with inadequate bandwidth resources. And—worst of all—SMBs are left using twentieth century business tools to try to create jobs in a twenty-first century global marketplace. This is no small issue.

The FCC could fix this problem simply and almost without cost by implementing relevant provisions of the Business Broadband Docket which have been languishing at the FCC for almost three years: the FCC should ensure the survival of a competitive market by requiring the giant phone companies to sell—at retail prices—the packet-based bandwidth necessary for technology competitors to provide cloud services to SMBs. Unleashing this existing broadband capacity for use by technology competitors at market-based rates will create an immediate cycle of investment, in-

novation and job creation by allowing our most entrepreneurial SMBs to do what they do best: focus on innovation rather than infrastructure.

Mr. Chairman and members of the Subcommittee, I appreciate the Committee's interest in this important topic and thank you for the opportunity to provide this statement for the record.