Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 23, *Issue* 3 2013 *Article* 7

VOLUME XXIII BOOK 3

Jurisdictional Challenges in the United States Government's Move to Cloud Computing Technology

Sasha Segall*

*Fordham University School of Law

Jurisdictional Challenges in the United States Government's Move to Cloud Computing Technology

Sasha Segall*

* Fordham University School of Law, J.D. Candidate, 2013; B.A., Journalism and Mass Communication, The George Washington University, 2010. I would like to thank Ryan Fox, Tiffany Miao, and the staff of IPLJ for their hard work in bringing this Note to print. A special thank you goes to my family, friends, and Sam for all of their love and support. The impetus for this Note comes from Professor Kerric Harvey, who initially sparked my interest and passion for discussing technology and security issues. Lastly, I would like to express my gratitude to Professor Aaron Saiger.

INTRODUCTION

President Barack Obama's 2008 election victory marked a paradigm shift in U.S. political history. For the first time, an American presidential campaign focused its efforts on new technology and the Internet.[1] In the months leading up to Election Day, the Obama campaign utilized several web-based applications, including Facebook, Myspace, and YouTube, to raise money, spread his political platforms, and, most importantly, establish a formidable base of young supporters.[2]

After being elected, President Obama continued to employ the technology-based tactics that had proven so useful during his campaign. Remnants of an antiquated system began to move out, and a surge of technology-based systems emerged. The most prominent change was the creation of two new administrative positions, the Chief Technology Officer ("CTO") and the Chief Information Officer ("CIO"). Their primary roles are to create changes to more efficiently utilize technology throughout government[3] and to oversee the government's extensive technological infrastructure, which includes twelve thousand major Information Technology systems and the hundreds of thousands of databases behind those systems.[4] As these databases host countless confidential federal documents, the officers' responsibilities cannot be understated.

On December 9, 2010, Vivek Kundra, President Obama's choice to serve as the nation's first CIO, mandated that all

---

1 Matthew Fraser & Soumitra Dutta, *Barack Obama and the Facebook Election*, U.S. NEWS & WORLD REPORT (Nov. 19, 2008), http://www.usnews.com/opinion/articles/2008/11/19/barack-obama-and-the-facebook-election ("[Obama] will be the first occupant of the White House to have won a presidential election on the Web.").

2 *Id*.

3 *See Technology*, THE WHITE HOUSE, http://www.whitehouse.gov/issues/technology (last visited Mar. 13, 2013 2:25 PM).

4 *Transparency and Federal Management IT Systems: Hearing Before the Subcomm. on Tech., Info. Policy, Intergovernmental Relations & Procurement Reform of the H. Comm. On Oversight & Gov't Reform*, 112th Cong. 7 (2011) (statement of Vivek Kundra, Federal Chief Information Officer, Office of Management and Budget) [hereinafter *Transparency and Federal Management IT Systems*].

government agencies "shift to [the] 'Cloud First' policy."[5] Most government agencies began this process by sharing their data with private corporations that offer Internet storage opportunities or cloud computing services.[6] Naturally, whenever the government changes the way in which it performs its daily business, those who work in government begin to recognize risks that may have been given little thought before the plan was implemented. In 2011, Vivek Kundra wrote in an op-ed article in the *New York Times* that "[o]ne of the critical remaining issues concerning cloud computing is whether cloud data can and should flow between nations and what restrictions should be placed upon it."[7] Although the motivation exists, and the financial resources are available to begin the transition, these security and privacy issues have not been resolved.

As the government increasingly relies on cloud computing technology to provide storage and perform computing tasks, voices from across the industry have raised concern over how these data servers will remain secure, governed, and protected. On May 25, 2011, Representative Sheila Jackson Lee remarked at a hearing before the Subcommittee on Intellectual Property, Competition, and the Internet that "the current trend of technology is to place information onto the cloud of third party operating systems and allows phones and computers to access this information. . . . [H]ow will the Government address jurisdictional issues? I don't want to ask about the Government, but what are you all doing with respect to that concept?"[8] These voices will continue to be heard as the

---

[5] VIVEK KUNDRA, THE WHITE HOUSE, 25 POINT IMPLEMENTATION PLAN TO REFORM FEDERAL INFORMATION TECHNOLOGY MANAGEMENT (2010), *available at* https://cio.gov/wp-content/uploads/downloads/2012/09/25-Point-Implementation-Plan-to-Reform-Federal-IT.pdf [hereinafter 25 POINT IMPLEMENTATION PLAN]. Steven VanRoekel, a former Microsoft executive, replaced Kundra as the new U.S. CIO on August 5, 2011 and remained dedicated to the 25 Point Plan. *See* Steven VanRoekel, *Shocking the System Through IT Reform*, THE WHITE HOUSE (June 7, 2012, 4:55 PM), http://www.whitehouse.gov/blog/2012/06/07/shocking-system-through-it-reform (discussing the successes of the Plan since its inception).

[6] *See infra* Part II.A.2.

[7] Vivek Kundra, *Tight Budget? Look to the "Cloud,"* N.Y. TIMES (Aug. 30, 2011), http://www.nytimes.com/2011/08/31/opinion/tightbudget-look-to-the-cloud.html?_r=1&.

[8] *Cybersecurity: Innovative Solutions to Challenging Problems: Hearing Before the Subcomm. on Intellectual Property, Competition, and the Internet of the H. Comm. On*

United States and its private data become "virtual" without concrete plans for protecting the security of our information.

Further, the location of data storage often has choice-of-law implications. If a data sever replicates one's information for safekeeping, multiple countries may have concurrent jurisdiction over the data server and subsequent legal disputes can occur.

This is not the first time in history that the government has been involved in jurisdictional challenges related to location and data security. After September 11, 2001, a United States program run by the Central Intelligence Agency and overseen by the Department of the Treasury used financial records to track and review the suspicious transactions of individuals suspected of having ties with Al Qaeda.[9] These international bank transactions were processed through the Society for Worldwide Interbank Financial Telecommunication ("SWIFT"), a Belgian cooperative.[10] "SWIFT operated two redundant data centers—one in the United States and one in the Netherlands," governed respectively by American and European law.[11] The Department of the Treasury exerted jurisdiction over all of SWIFT's data through its authority over the U.S. center.[12]

The Treasury program was publicly disclosed in 2006, leading many Europeans to claim that "American access to European banking data violated European data privacy laws."[13] "European authorities compelled SWIFT to bifurcate [the] data storage, keeping European data exclusively on the Netherlands [sic] server" so as to subject the data to European privacy regulation.[14]

the Judiciary, 112th Cong. 85 (2011) (statement of Rep. Sheila Jackson Lee, Member, H. Comm. On the Judiciary).

9 *See* Eric Lichtblau & James Risen, *Bank Data Is Sifted by U.S. in Secret to Block Terror*, N.Y. TIMES (June 23, 2006), http://www.nytimes.com/2006/06/23/washington/23intel.html?pagewanted=1.

10 *See id*.

11 Michael Chertoff, *Data Sovereignty in the Cloud: The Issues for Government*, SAFEGOV (Nov. 1, 2011), http://safegov.org/2011/11/1/data-sovereignty-in-the-cloud-the-issues-for-government.

12 *Id*.

13 *Id*.

14 *Id*.

As one can see, the location of data storage often implicates choice-of-law considerations. If a data server replicates one's information for safekeeping, multiple countries may have concurrent jurisdiction over the data server and subsequent legal disputes can occur.

This Note proceeds in three parts. Part I introduces cloud computing technology, the U.S. government's move to cloud computing, the present state of U.S. jurisdictional law, and international regulations governing data and privacy. Part II examines how international regulations governing cloud computing technology differ from regulations in the United States. Part II also illustrates several conflicts that could arise if the United States does not increase its regulation of the cloud computing industry. Finally, Part III proposes two solutions to achieve security while the U.S. government moves to cloud computing. The government should either maintain data centers on its own property and contract out its technological needs, or else adopt a cohesive regulatory system that emulates the European Union's by requiring that government data be maintained domestically, even if not specifically on government owned property.

I. BACKGROUND

This Part provides a background for understanding how cloud computing raises jurisdictional questions, thereby affecting control and access to data. Part I.A discusses the history and current infrastructure of cloud computing technology. Part I.B explains the U.S. government's shift to cloud computing technology. Part I.C explores the effect of U.S. jurisdictional law on cloud computing, while Part I.D discusses the international approach to regulating data.

A. What's in a Name: The Present State of Cloud Computing

1. The Definition and History of Cloud Computing

"Cloud computing" is a misnomer. On its face, the term "cloud" suggests that when a user composes an e-mail and clicks "send," the e-mail floats up and is stored somewhere in the sky. In

reality, the opposite is true. While satellites often transmit data for the purposes of cloud computing, technology companies that offer cloud computing services store and process data on the ground in massive "server farms."[15] These server farms contain hundreds of thousands of individual servers.[16] When a user accesses data stored on a server, it is referred to as using cloud computing technology.[17]

The term "cloud computing" was first developed in the 1960s when corporations used a cloud symbol to represent the Internet during business meetings.[18] However, it was not publicly used to describe an approach to data storage until August 2006 when Google CEO Eric Schmidt first publicly used the term at a search engine conference in San Jose, California.[19] According to a news report by NBC, this may have been an early start to the Google-Amazon "Internet wars," as Schmidt may have been trying to pre-empt Amazon's Elastic Compute Cloud system, which was released that same month.[20]

Cloud computing can be defined as a "computing model" used to deliver information technology and computing services through the Internet,[21] to store data, or to offer services such as virtual

---

15 Paul T. Jaeger, Jimmy Lin, Justin M. Grimes, & Shannon N. Simmons, *Where is the Cloud? Geography, Economics, Environment, and Jurisdiction in Cloud Computing*, 14 FIRST MONDAY 1, § 4 (2009), *available at* http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2456/2171.

16 *Id*. While larger companies, such as Amazon and Google, are able to maintain their own server farms, "[m]any companies rent space in shared (or 'co-location') centers belonging to" larger companies. *Not a Cloud in Sight*, ECONOMIST (Oct. 27, 2012), http://www.economist.com/news/special-report/21565003-best-places-store-your-terabytes-not-cloud-sight.

17 *See* Mark Koba, *Cloud Computing: CNBC Explains*, CNBC (June 29, 2011, 11:30 AM), http://www.cnbc.com/id/43483060/Cloud_Computing_CNBC_Explains ("In simplest terms, cloud computing involves delivering hosted services over the Internet. The service end is where the data or software is stored and the user end is a single person or company network.").

18 *Id*.

19 *Id*.

20 *Id*.

21 *See* Vivek Kundra, *Streaming at 1:00: In the* Cloud, THE WHITE HOUSE (Sept. 15, 2009, 12:09 PM), http://www.whitehouse.gov/blog/streaming-at-100-in-the-cloud.

desktops, which allow remote access to data.[22] Before cloud computing, a computer could only run software that was installed on its hard drive, and a computer's capabilities were limited to the data and processing power contained therein.[23] For example, in the 1990s, users who wanted to use the AOL Instant Messenger ("AIM") application were required to install software from a CD onto their computers to access the application.[24]

Cloud computing has revolutionized how users interact with software by allowing a computer to serve as simply the front-end portal, an access point through which users access software and data on remote servers. Today's version of AIM—Google Chat, the instant message feature of Google's Gmail—does not require users to load or download software; instead, the program initiates once a user accesses the program through Gmail.[25] Among other advantages of cloud computing, users can access vastly larger stores of data and greater processing power through cloud computing than their personal computers would otherwise allow.[26]

2. Daily Interactions with Cloud Computing

In this age of robust technology, a majority of the U.S. population has used cloud computing in one way or another.[27] According to the U.S. Census Bureau's 2011 Current Population Survey, seventy-eight percent of American adults use the

---

[22] Richard Spires, *Cloud Computing, Front and Center*, CIOC BLOG (Sept. 6, 2011), https://cio.gov/cloud-computing-front-and-center.

[23] *See* Michael Miller, *Cloud Computing Pros and Cons for End Users*, QUE PUBLISHING (Feb. 13, 2009), http://www.quepublishing.com/articles/article.aspx?p=1324280.

[24] *See Burn-Your-Own-AOL-CD*, AOL HELP, http://help.aol.com/help/microsites/search.do?cmd=displayKC&externalId=223798#fourth ("The AOL Installer CD is no longer available at a retail store . . . .").

[25] *About Chatting in Gmail*, GOOGLE, http://mail.google.com/mail/help/chat.html (last visited Feb. 12, 2012).

[26] *See* Miller, *supra* note 23; *see also* JOHN VILLASENOR, CENTER FOR TECHNOLOGY INNOVATION AT BROOKINGS, ADDRESSING EXPORT CONTROL IN THE AGE OF CLOUD COMPUTING 1 (Christine Jacobs ed., 2011), *available at* http://www.brookings.edu/~/media/Files/rc/papers/2011/0725_cloud_computing_villasenor/0725_cloud_computing_villasenor.pdf.

[27] *The PC Generation: Computer Use, 2000*, U.S. CENSUS BUREAU (2010), http://www.census.gov/population/pop-profile/2000/chap10.pdf.

Internet.[28] This often requires interfacing with cloud computing technology. Any AOL, Hotmail, Yahoo Mail, or Gmail user has interacted with cloud computing technology.[29] Further, each of the 300 million photographs uploaded to Facebook every day represents an interaction with cloud computing technology.[30] Industry research predicts that the cloud computing market will swell to a $241 billion industry by 2020.[31]

Cloud computing services can be broken down into three main service models: Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS).[32] SaaS includes blogs, applications available on a smartphone or tablet,[33] and any software that can be accessed through a web browser, such as Email as a Service (EaaS).[34] SaaS powers all of Google's

---

[28] *See Adult Computer and Adult Internet Users by Selected Characteristics: 2000 to 2011*, U.S. CENSUS BUREAU (2012), http://www.census.gov/compendia/statab/2012/tables/12s1158.pdf; *see also Digital Nation: Expanding Internet Usage*, U.S. DEP'T. OF COMMERCE, NAT'L TELECOMM. & INFO. ADMIN. (2011), *available at* http://www.ntia.doc.gov/files/ntia/publications/ntia_internet_use_report_february_2011.pdf ("As a group, an estimated 209 million Americans—about 72 percent of all adults and children ages three years and older—use the Internet *somewhere*, whether it be at home, the workplace, schools, libraries, or a neighbor's house.").

[29] *See, e.g.*, Aaron Lake & Jacob Rosenberg, *You've Got . . . AOL Cloud Computing*, UPTIME INSTITUTE, http://symposium.uptimeinstitute.com/advanced-search/1234-youve-got-aol-cloud-computing (last visited Mar. 13, 2013).

[30] *See* Loek Essers, *Facebook to Use 'Cold Storage' to Deal with Vast Amounts of Data*, INFOWORLD (Oct. 17, 2012), http://www.infoworld.com/d/cloud-computing/facebook-use-cold-storage-deal-vast-amounts-of-data-205127.

[31] *Forrester Forecasts USD 241 Billion Cloud Computing Market By 2020*, INFORMATION WEEK (Apr. 26, 2011), http://www.informationweek.in/Cloud_Computing/11-04-26/Forrester_forecasts_USD_241_billion_cloud_computing_market_by_2020.aspx.

[32] Vivek Kundra, *Federal Cloud Computing Strategy*, THE WHITE HOUSE 6 (2011), https://cio.gov/wp-content/uploads/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf.

[33] *See* Gianpaolo Carraro & Fred Chong, *Software as a Service (SaaS): An Enterprise Perspective*, MSDN (Oct. 2006), http://msdn.microsoft.com/en-us/library/aa905332.aspx ("Simply put, SaaS can be defined as—software deployed as a hosted service and accessed over the Internet.").

[34] *See Email as a Service (EaaS)*, INFO.APPS.GOV, http://www.info.apps.gov/content/email-service-eaas-0 (last visited Mar. 13, 2013) (explaining how E-mail as a service virtually delivers an e-mail program to your computer without the need for a software program).

applications, or "Apps,"[35] such as Gmail, Google Calendar, Google Docs, and Google Drive.[36] Today, when a user logs into Gmail, Google's e-mail program, the user accesses e-mail through a remote Google program that has not been installed on the user's computer.[37] When the user sends an e-mail to another user through Gmail, Google stores that data on its data server until the recipient opens the e-mail, thereby drawing information from the data server onto the user's monitor.[38] Every time a user accesses the restaurant reservation website OpenTable, uses Adobe services, or takes a survey through Survey Monkey, she is accessing a SaaS platform.

IaaS provides virtual hardware storage for corporations and government users, such as Amazon web services.[39] PaaS includes a platform for accessing other cloud software—an example is Facebook.[40]

Data servers that store private, business, and governmental information are located all over the world.[41] These server farms

---

[35] Wesley Chun, *What is Cloud Computing?*, GOOGLE DEVELOPERS (June 2012), https://developers.google.com/appengine/training/intro/whatiscc ("Another example of SaaS from Google includes their Apps product: office productivity software hosted and run by Google online.").

[36] *Google Apps for Business*, GOOGLE, http://www.google.com/enterprise/apps/business/index21.html?utm_expid=65468332-15&utm (last visited Mar. 29, 2013).

[37] *See Supported Browsers*, GOOGLE, http://support.google.com/mail/bin/answer.py?hl=en&answer=6557 (last updated Dec. 28, 2012) (stating that a user must use an Internet browser to access all Google remote programs such as Gmail).

[38] *See What Happens to Messages Stored on Gmail's Servers?*, GOOGLE, http://support.google.com/mail/bin/answer.py?hl=en&answer=13288&topic=1668962&ctx=topic (last updated Oct. 16, 2012).

[39] *See* Chun, *supra* note 35.

[40] *See Cloud Computing*, MICROSOFT, http://www.microsoft.com/industry/government/guides/cloud_computing/5-PaaS.aspx ("With Platform as a Service (PaaS), you can develop new applications or services in the cloud that do not depend on a specific platform to run, and you can make them widely available to users through the Internet."); *see also* David Kirkpatrick, *Facebook's Changes—It's All About the Platform*, FORBES (Sept. 22, 2011, 5:54 PM), http://www.forbes.com/sites/techonomy/2011/09/22/facebooks-changesits-all-about-the-platform; Phil Wainewright, *Is Facebook a Paas Contender?*, ZDNET (Apr. 11, 2008, 5:07 PM), http://www.zdnet.com/blog/saas/is-facebook-a-paas-contender/488.

[41] *See* Mark Prigg, *Inside the Internet: Google Allows First Ever Look at the Eight Vast Data Centres that Power the Online World*, MAILONLINE (Oct. 17, 2012, 1:22 PM),

are extraordinarily costly to run and power.[42] As a result, American companies seek to reduce the operating costs of cloud computing technology by locating these servers outside of the United States.[43] For instance, Amazon has data servers located in São Paulo, Amsterdam, Dublin, Frankfurt, London, Paris, Stockholm, Hong Kong, Singapore and Tokyo.[44] Google, having long kept their servers' locations discreet, has recently revealed some information about the locations of their data centers.[45] Facebook opened an enormous server farm, the size of eleven football fields, in Luleå, Sweden to take advantage of the cold climate and to lower the costs associated with cooling down data servers.[46] Amazon, Google, and Facebook are just three of the many corporations that provide cloud computing services and store their data servers worldwide.

3. Data Replication as a Way of Protecting Information

There are also environmental risks associated with the location and maintenance of data servers. In December 2011, Microsoft's cloud computing program Azure reported that their data centers

http://www.dailymail.co.uk/sciencetech/article-2219188/Inside-Google-pictures-gives-look-8-vast-data-centres.html (last updated Oct. 19, 2012).

42 *See* Richard Orange, *Global Server Farms Around the World*, THE TELEGRAPH (Oct. 26, 2011, 4:04 PM), http://www.telegraph.co.uk/technology/facebook/8850861/Global-server-farms-around-the-world.html.

43 *See* Veronique Greenwood, *Move Server Farms to Desert? Data is Easier to Move Than Power, After All*, DISCOVER (Apr. 27, 2011, 12:08 PM), https://blogs.discovermagazine.com/80beats/2011/04/27/move-server-farms-to-desert-data-is-easier-to-move-than-power-after-all/#.UVNaWaV4sW9 ("Keeping all those servers cool has been said to eat up 50% of the electricity such centers need—in fact, Iceland has proposed that its chilly climate makes it an ideal place for server farms."); Richard Orange, *Facebook to Build Server Farm on Edge of Arctic Circle*, TELEGRAPH (Oct. 26, 2011, 2:47 PM), http://www.telegraph.co.uk/technology/facebook/8850575/Facebook-to-build-server-farm-on-edge-of-Arctic-Circle.html.

44 *Amazon CloudFront*, AMAZON WEB SERVICES, http://aws.amazon.com/cloudfront/; *Amazon Simple Storage Service (Amazon S3)*, AMAZON WEB SERVICES, http://aws.amazon.com/s3; Rich Miller, *Where Amazon's Data Centers Are Located*, DATA CENTER KNOWLEDGE (Nov. 18, 2008), http://www.datacenterknowledge.com/archives/2008/11/18/where-amazons-data-centers-are-located.

45 *See* Prigg, *supra* note 41; *see also Data Center Locations*, GOOGLE, http://www.google.com/about/datacenters/inside/locations (last visited Apr. 4, 2013) (listing the domestic and international location of thirteen data centers in the Americas, Asia and Europe).

46 *See* Orange, *supra* note 43.

lose power and information 11.1 times per month due to electrical outages.[47] This risk is especially prevalent in areas prone to natural disasters.[48] The production of data server components, which often takes place in these risk-prone areas, further threatens the functionality of server farms. For example, the *New York Times* reported that, in November 2011, flooding forced factories producing hard drives in Thailand to shut down.[49] These hard drives are necessary to store data in cloud computing centers.[50] Thailand's estimated production loss was thirty percent of its annual output, or fifty million hard drives.[51] With the booming cloud computing industry already operating at a ninety percent production output, the Thailand disaster posed a marked threat to companies such as Western Digital, one of the world's biggest storage companies.[52]

To protect against data loss, Google and Amazon have been using data replication systems.[53] Through data replication, information is replicated and then stored in multiple locations to

---

[47] Andrew R. Hickey, *Amazon, Microsoft Top Short List of Cloud Storage Providers: Study*, CRN (Dec. 9, 2011, 11:40 AM), http://www.crn.com/news/cloud/232300242/amazon-microsoft-top-short-list-of-cloud-storage-providers-study.htm;jsessionid=HBnfEdtD4F0qsPfqVY5Eog**.ecappj01?pgno=1.

[48] *See* Lori MacVittie, *Cloud Computing: Location Is Important, but not the Way You Think*, DEVCENTRAL (Jan. 21, 2009), http://devcentral.f5.com/weblogs/macvittie/archive/2009/01/21/cloud-computing-location-is-important-but-not-the-way-you.aspx.

[49] Nick Bilton, *Thailand Floods Could Affect Cloud Computing*, N.Y. TIMES (Nov. 4, 2011, 9:45 AM), http://bits.blogs.nytimes.com/2011/11/04/thailand-floods-will-affect-computer-makers-and-web-sites/?scp=1&sq=cloud%20computing&st=cse.

[50] *See id.*

[51] *See id.*

[52] *See id.* ("Component makers in China, the Philippines and Malaysia could pick up some of the slack, but many global hard drive makers are already operating at over 90 percent production, with some in China at 98 percent."); Dean Takahashi, *WD Resumes Hard Drive Production After Thailand Floods*, VENTUREBEAT (Dec. 1, 2011, 6:39 PM), http://venturebeat.com/2011/12/01/wd-resumes-hard-drive-production-after-thailand-floods.

[53] *See Amazon Relational Database Service (Amazon RDS)*, AMAZON WEB SERVICES, http://aws.amazon.com/rds/ (last visited Mar. 13, 2013) ("Amazon RDS automatically patches the database software and backs up your database, storing the backups for a user-defined retention period and enabling point-in-time recovery."); *see also Disaster Recovery by Google*, GOOGLE (Mar. 4, 2010), http://googleenterprise.blogspot.com/2010/03/disaster-recovery-by-google.html.

ensure that the information is always accessible and secure in the event of disaster or intentional destruction.[54]

B. The U.S. Government's Plan for Cloud Computing

The federal government is among the greatest spenders on technology in the United States.[55] Each year, the government spends $80 billion dollars on information technology.[56] As such, when Vivek Kundra, the former U.S. Chief Information Officer (CIO), joined the Obama Administration, one of his main objectives was the promotion of efficient and effective use of the federal information technology budget.[57] Inefficiencies in the system ranged from having thousands of inactive websites to having more than ten thousand separate information technology systems that were idle ninety-three percent of the time.[58] Kundra, who unsurprisingly also fought to make President Obama the first president to receive a smartphone, started consolidating these IT systems—marking the government's shift towards cloud computing systems.[59]

At the Forum on Information Technology Management Reform in December 2010, Kundra released his "25 Point Implementation Plan to Reform Federal Information Technology Management."[60] The eighteen-month plan proposed a three-step "Cloud First" policy for all federal agencies.[61] The Cloud First policy required

---

54 *See* Danny Bradbury, *Remote Replication: Comparing Data Replication Methods*, COMPUTERWEEKLY.COM, http://www.computerweekly.com/feature/Remote-replication-Comparing-data-replication-methods ("Remote replication copies data to a secondary site as part of a disaster recovery plan; it traditionally involved backing up application data, but it is now possible to replicate entire virtual machines too. This can be useful to maintain server images with the latest configuration, including operating system and application security patches that are all set to be made live in case of a serious outage at the primary site.").

55 Geoff Colvin, *Uncle Sam's First CIO*, FORTUNE MAGAZINE (July 13, 2011, 3:37 PM), http://money.cnn.com/2011/07/13/news/companies/vivek_kundra_leadership.fortune/index.htm ("The U.S. government is the world's largest consumer of information technology . . . .").

56 *Id.*

57 *See Transparency and Federal Management IT Systems*, *supra* note 4.

58 *See* Colvin, *supra* note 56.

59 *Id.*

60 25 POINT IMPLEMENTATION PLAN, *supra* note 5, at 1.

61 *Id.*

the agencies to use cloud computing instead of buying hardware and software.[62] Under Cloud First, agencies had an obligation to identify three "must move" services by March 2010, and to move one of these to the cloud by December 2010, and to then move the remaining two services to the cloud by June 2011.[63] Kundra predicted that the U.S. government would save at least five billion dollars by using cloud computing instead of the old hard-copy storage system.[64]

On February 8, 2011, Kundra released the "Federal Cloud Computing Strategy," which further explains the role of cloud computing in federal agencies and outlines his expectations under the Cloud First policy.[65] Cloud First imposes many new technological requirements on federal agencies. Each agency has its own designated Chief Information Officer, who is tasked with carrying out the 25 Point Plan and ensuring that its requirements are met.[66] The CIO of each federal agency is also responsible for ensuring a "safe, secure cloud solution" and for overseeing the allocation of funds.[67] Cloud First also requires each agency to "[d]etermine cloud readiness" and ensure that the security requirements are met.[68] To comply with these security requirements, CIOs must look at "[s]tatutory compliance to laws, regulations, and agency requirements," privacy and confidentiality, integrity, and "[d]ata controls and access policies to determine where data can be stored and who can access physical locations."[69]

---

62 25 POINT IMPLEMENTATION PLAN, *supra* note 5, at 1. *See also* David Saleh Rauf, *Stakes High for Cloud Contractors*, POLITICO (Sept. 18, 2011, 10:54 PM), http://www.politico.com/news/stories/0911/63786.html#ixzz1bAXu6nqE.

63 25 POINT IMPLEMENTATION PLAN, *supra* note 5, at 1.

64 *See* Kim Hart, *Vivek Kundra Leaving White House for Harvard*, POLITICO (June 16, 2011, 9:37 AM), http://www.politico.com/news/stories/0611/57115.html.

65 VIVEK KUNDRA, THE WHITE HOUSE, FEDERAL CLOUD COMPUTING STRATEGY 2 (2011), *available at* http://ctovision.com/wp-content/uploads/2011/02/Federal-Cloud-Computing-Strategy1.pdf [hereinafter FEDERAL CLOUD COMPUTING STRATEGY].

66 *See* Steven VanRoekel, *The Changing Role of Federal Chief Information Officers*, THE WHITE HOUSE (Aug. 8, 2011, 6:22 PM), whitehouse.gov/blog/2011/08/08/changing-role-federal-chief-information-officers.

67 *See* FEDERAL CLOUD COMPUTING STRATEGY, *supra* note 65, at 13.

68 *Id*.

69 *Id*. at 14.

Cloud First utilizes the General Services Administration ("the GSA"), the National Institute of Standards and Technology (the "NIST"), the Department of Homeland Security (the "DHS"), and the Office of Management and Budget (the "OMB") to help agencies "efficiently acquire cloud computing capabilities and mitigate threats."[70] The NIST and the GSA are responsible for creating cloud computing standards, giving guidance to the agencies, and developing contracts with suppliers.[71] The DHS is responsible for monitoring security issues related to cloud computing.[72] To coordinate all of these agencies and offices, the OMB provides guidance as the agencies transition to cloud computing.[73]

Additionally, Cloud First mandates that agencies form contracts with private technology companies.[74] To streamline the approval process for cloud service providers, the government plans to use an "approve once and use often" approach.[75] Besides big players in the cloud service provider industry—Amazon, Dell, Microsoft, and Google—there are many smaller private technology companies that have contracted with the government to develop the cloud computing industry.[76] Each CIO has a massive IT budget to fund the transition to cloud computing.[77] For example, the Honorable Roger Baker, the CIO for the Department of Veteran Affairs, currently operates a three billion dollar budget, largely supporting the health and benefits administration.[78]

C. U.S. Jurisdictional Policies and the Effect of these Policies on Cloud Computing

The dynamic nature of the cloud computing industry creates a system in which data originating in one country passes through and is stored within several foreign jurisdictions, sometimes

---

70 *Id*. at 25.
71 *See id*. at 31.
72 *See id*.
73 *See id*.
74 *See id.* at 16.
75 *Id.* at 28.
76 *See* Rauf, *supra* note 62.
77 *See* FEDERAL CLOUD COMPUTING STRATEGY, *supra* note 65, at 35.
78 *Transparency and Federal Management IT Systems*, *supra* note 4, at 17.

simultaneously.[79] As the SWIFT incident demonstrated earlier, the multi-jurisdictional nature of cloud computing creates issues for determining what state or country may have access to data stored on a server. Courts must determine the law that should apply when resolving cloud computing disputes and, as a threshold matter, whether the court can even hear the dispute.[80] The Federal Rules of Civil Procedure dictate that a court must be able to exercise personal jurisdiction over a defendant for that defendant to be properly brought before the court.[81] Once in court, choice of law principles govern which law applies: the law of the state in which the subject of the lawsuit occurred, or that of the state in which the court sits.[82]

1. U.S. Personal Jurisdiction

In the United States, personal jurisdiction is governed by the U.S. Supreme Court's interpretation of the Due Process Clause of the Fourteenth Amendment. The Due Process Clause prevents any State from "depriv[ing] any person of life, liberty, or property, without due process of law."[83] Due process protects a person's right "to be subject only to lawful power," which includes protecting litigants from having to defend lawsuits in arbitrary locations.[84] To assert jurisdiction over an out-of-state corporation, the Court held in *International Shoe Co. v. Washington* that due process requires (1) that the defendant have certain minimum contacts with the forum state and (2) that compelling the defendant

---

79 Kristina Irion, *Government Cloud Computing and the Policies of Data Sovereignty*, 22ND EUROPEAN REGIONAL CONFERENCE OF THE INTERNATIONAL TELECOMMUNICATIONS SOCIETY 10 (Sept. 18–21, 2011), https://www.econstor.eu/dspace/bitstream/10419/52197/1/672481146.pdf.

80 *See* VILLASENOR, *supra* note 26, at 2 (stating that "the cloud raises complex policy questions of security . . . privacy . . . and jurisdiction . . . [and that] [i]f data that falls within a category subject to U.S. export control regulations ends up on a server in Europe, the question of whether or not a violation of U.S. export control laws has occurred will often turn in large part on the question of whether that data travelled there from the United States").

81 *See* FED. R. CIV. P. 12(b)(2).

82 Christopher A. Whytock, *Myth of Mess? International Choice of Law in Action*, 84 N.Y.U. L. REV. 719, 724 (2009).

83 U.S. CONST. amend. XIV, § 1.

84 J. McIntyre Mach., Ltd. v. Nicastro, 131 S. Ct. 2780, 2789 (2011).

to defend in that state would not "offend traditional notions of fair play and substantial justice."[85] Hence, a defendant's actions, not his expectations, give a state's courts jurisdiction over him.[86]

Since *International Shoe*, the Court has differentiated between specific jurisdiction and general jurisdiction.[87] A court has "specific jurisdiction" over a defendant when the suit "aris[es] out of or [is] related to the defendant's contacts with the forum."[88] Specific jurisdiction includes purposeful availment, in which a defendant has conducted activity within a state and has thus invoked the benefits and protections of that state's laws.[89] A state's court has general jurisdiction over a defendant when, although the suit did not "aris[e] out of [and is not] related to the defendant's contacts with the forum,"[90] the defendant has had "continuous and systematic" contacts with the state that "render [him] essentially at home in the forum State."[91]

2. Personal Jurisdiction over the Internet and Through Data Servers

The Supreme Court has found that technological advancements call for the redefinition of traditional personal jurisdiction doctrine.[92] In *Hanson v. Denckla*, Chief Justice Earl Warren stated that "as technological progress has increased the flow of commerce between States, the need for jurisdiction over nonresidents has

---

85 Int'l Shoe Co. v. Washington, 326 U.S. 310, 316 (1945) (quoting Milliken v. Meyer, 311 U.S. 457, 463). International Shoe Co. was a Delaware corporation with its principal place of business in St. Louis, Missouri. *Id.* at 313. International Shoe Co. hired salesmen who resided in Washington. *Id.* Washington State brought a suit against International Shoe Co. in Washington state court to recover unpaid contributions to state unemployment compensation fund. *Id.* at 311–12.

86 *J. McIntyre Mach.*, 131 S. Ct. at 2790 ("[The] facts may reveal an intent to serve the U.S. market, but they do not show that J. McIntyre purposefully availed itself of the New Jersey market.").

87 Helicopteros Nacionales de Colombia, S.A. v. Hall, 466 U.S. 408, 414 n.8 (1984).

88 *Id.*

89 Hanson v. Denckla, 357 U.S. 235, 253 (1958) ("[I]t is essential in each case that there be some act by which the defendant purposefully avails itself of the privilege of conducting activities within the forum State, thus invoking the benefits and protections of its laws.").

90 *Helicopteros*, 466 U.S. at 415 n.9.

91 Goodyear Dunlop Tires Operations v. Brown, 131 S. Ct. 2846, 2851 (2011).

92 *Hanson*, 357 U.S. at 250–51.

undergone a similar increase."[93] At first lower courts struggled to establish jurisdictional boundaries within the Internet's virtual space. In *Bensusan Restaurant Corp. v. King*, Second Circuit Judge Van Graafeiland stated, "attempting to apply established [ ] law in the fast-developing world of the internet is somewhat like trying to board a moving bus."[94] However, as Internet transactions have developed into a distinct business and social marketplace, there has been an increasing amount of judicial precedent as to the ways a court can establish jurisdiction based on a user's Internet activities.[95]

Many courts have found that server location—where the processing of information occurs—implicates a valid state interest.[96] For example, in 2007, the Eastern District of Virginia, in a union dispute case over e-mails sent to Verizon, held that the location of the corporation's data server, along with the location of some of its employees who received the e-mails, was sufficient to establish jurisdiction in Virginia.[97] In 2012, the Second Circuit explored the question of whether a Connecticut court could exercise jurisdiction over a defendant who, while living and working in Canada, accessed a computer data server in

---

93 *Id*.

94 126 F.3d 25, 27 (2d Cir. 1997).

95 *See, e.g.*, Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1124 (W.D. Pa. 1997) (applying a sliding-scale test of commercial interactivity to measure an Internet user's level of engagement with a particular website, which essentially established a threshold for whether a user has "purposefully availed" themselves to a state based on their Internet activity). The Western District of Pennsylvania created the *Zippo* test in response to the jurisdictional problems created by the Internet. *See id*. Many circuit courts rely on the *Zippo* test for guidance in determining when a court can properly claim specific jurisdiction over a user. *See e.g.*, Best Van Lines, Inc. v. Walker, 490 F.3d 239, 251 (2d Cir. 2007) ("In analyzing personal jurisdiction in the internet context, many courts have turned to the standards set out more than ten years ago by a judge of the Western District of Pennsylvania in *Zippo* . . . ."); Toys "R" Us, Inc. v. Step Two, S.A., 318 F.3d 446, 452 (3d Cir. 2003) (describing *Zippo* as the "seminal authority regarding personal jurisdiction based upon the operation of an Internet web site"); ALS Scan, Inc. v. Digital Serv. Consultants, Inc., 293 F.3d 707, 713 (4th Cir. 2002) (adopting the *Zippo* test).

96 Joel R. Reidenberg, *Technology and Internet Jurisdiction*, 153 U. PA. L. REV. 1951, 1962 (2005).

97 *See* Aitken v. Commc'ns Workers of Am., 496 F. Supp. 2d 653, 659 (E.D. Va. 2007).

Connecticut in connection with illegal activity.[98] The District Court had dismissed the complaint for lack of personal jurisdiction.[99] The Second Circuit held that jurisdiction is "reasonable" as the defendant "purposefully availed herself of the privilege of conducting activities within Connecticut" and "[i]t is not material that [the defendant] was outside of Connecticut when she accessed the . . . servers."[100]

When U.S. courts try to establish jurisdiction over international cases, it is difficult to establish proper jurisdiction because United States laws often conflict with the laws of other countries. In *Yahoo! Inc. v. La Ligue Contre Le Racisme et L'antisemitisme* ("LICRA"), the Ninth Circuit heard a case that involved both U.S. and French law.[101] At the time of the suit, Yahoo was incorporated in Delaware, had data servers in California, and foreign subsidiaries in France, the UK, and India.[102] The website Yahoo.com provided a user platform for Nazi discussions and auction information.[103] Activity such as this is unlawful under the French Criminal Code, which bans the exhibition and sale of Nazi propaganda.[104] LICRA sent a cease and desist letter to Yahoo in France, ordering Yahoo to take the Nazi paraphernalia off the Internet.[105] The letter was followed by interim orders from a French court demanding that Yahoo remove the anti-Semitic content from its website.[106] The French court held Yahoo liable under the French penal code because the illegal content was *viewed* in France.[107] Yahoo argued that it did not have the technology to remove the content from its French site without affecting its U.S. site.[108]

98 MacDermid, Inc. v. Deiter, 702 F.3d 725, 726–27 (2d Cir. 2012).
99 *Id*. at 727.
100 *Id*. at 729–30.
101 *See* 433 F.3d 1199, 1201 (9th Cir. 2006).
102 *Id*. at 1201–02.
103 *Id*. at 1202.
104 *See id*. at 1221.
105 *Id*. at 1232 (Tashima, J., concurring).
106 *Id*.
107 *Id*. at 1225 (Ferguson, J., concurring).
108 *Id.* at 1203.

Yahoo reacted by filing suit in a U.S. district court, claiming that the French interim orders were not enforceable in the United States.[109] Yahoo alleged that LICRA could not hold Yahoo liable in the United States due to First Amendment protections.[110] The U.S. district court found that the decision by the French court was inconsistent with the First Amendment to the Constitution, and therefore, the French court's decision was inapplicable in the United States.[111]

LICRA then appealed the case to the U.S. Court of Appeals for the Ninth Circuit.[112] Ultimately, the Ninth Circuit reversed portions of the earlier holding but maintained that the U.S. district court had personal jurisdiction over the French defendants.[113] The French court order was left unenforced despite the violation of French law.[114] Yahoo then decided to remove the Nazi paraphernalia from its website entirely.[115] This is just one example of the United States' problem of territorial jurisdiction when conflicts involving international law arise.[116]

3. Choice of Law Doctrine as Applied in the United States

Choice of law is the doctrine used to determine which body of law applies in a dispute between parties from different states or countries.[117] As the SWIFT incident demonstrated, when the EU had a conflict with the United States regarding international financial data, it became unclear which jurisdiction would govern

---

109 *Id.* at 1204.

110 *Id*. at 1206.

111 *Id.* at 1204–05.

112 *Id*. at 1205.

113 *See id*. at 1201.

114 *See id*. ("The district court held that . . . the French orders are not enforceable in the United States because such enforcement would violate the *First Amendment*. . . . LICRA and UEJF appeal only the personal jurisdiction, ripeness, and abstention holdings.").

115 Susan Dodson, *The Very Long Arm of the Law*, THE GUARDIAN (Nov. 9, 2001, 1:15 PM), http://www.guardian.co.uk/technology/2001/nov/09/internetnews.

116 *See* Joel R. Reidenberg, *Yahoo and Democracy on the Internet*, 42 JURIMETRICS J. 261, 271 ("The cases reveal that, to the extent that an Internet actor strives to target users in a foreign jurisdiction, the foreign forum can assert territorial jurisdiction and apply the forum's law. While a number of the cases involved protecting the intellectual property of parties in the forum, the vice cases illustrate that the principle applies equally to issues of public order. Courts assert territorial jurisdiction to protect values held in the forum.").

117 Whytock, *supra* note 82, at 724.

the dispute. Ultimately, the United States negotiated an agreement with the EU, leaving this issue undecided.[118]

Choice of law issues are critical in the cloud computing context as many service providers use data replication to store the same information in many jurisdictions. This practice creates uncertainty as to which law would apply; however, the problem can be ameliorated with a simple choice of law provision in the underlying contract.

The U.S. Constitution requires a state to enforce proceedings of other states, limit the jurisdiction of a state's courts, prevent a state from discriminating against citizens of another state, give effect to the Constitution, statutes, and treaties of the United States, and limit a state's power to apply local law in interstate commerce.[119] There is no uniform choice of law rule in the United States; instead, each state has its own choice of law provisions.[120] Some states mandate that the law where an incident occurred governs the case, while other states always use their own laws.[121]

Today, due to the different state or international laws that can be involved in a single contract, many contracts include a choice of law provision that dictates what law will apply should a contract dispute arise.[122] The Restatement of Conflict of Laws permits contracting parties to choose a governing law, but if the contract

---

118 *See Terrorist Finance Tracking Center*, U.S. DEP'T OF THE TREASURY (last visited Mar. 16, 2013), http://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Pages/tftp.aspx ("At the end of 2009 SWIFT stopped storing certain sets of these critical data on its U.S. servers and hosts those data in the European Union. The United States negotiated an agreement with the European Union on the processing and transfer of this information to the U.S. Treasury Department. The Agreement became effective on August 1, 2010.").

119 *See* U.S. CONST. amend. XIV, § 1.

120 Whytock, *supra* note 82, at 724.

121 *See* RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 6 cmt. b (1971) ("The court should give a local statute the range of application intended by the legislature when these intentions can be ascertained and can constitutionally be given effect. If the legislature intended that the statute should be applied to the out-of-state facts involved, the court should so apply it unless constitutional considerations forbid. On the other hand, if the legislature intended that the statute should be applied only to acts taking place within the state, the statute should not be given a wider range of application.").

122 *See id*. at cmt. g ("[T]he parties are free within broad limits to choose the law to govern the validity of their contract.").

does not cover a particular issue, there are opportunities for parties to circumvent the choice-of law provisions.[123]

These choice-of-law provisions are prevalent in business and government contracts. Public cloud computing companies like Amazon, Microsoft, Rackspace, and Google—as well as private companies such as Eucalyptus—require anyone who uses their services to agree to contracts governing technology services.[124] Many of the contracts between the service providers and users who purchase these services include choice-of-law provisions. For example, Amazon Web Service mandates that:

> The laws of the State of Washington, without reference to conflict of law rules, govern this Agreement and any dispute of any sort that might arise between you and us. Any dispute relating in any way to the Service Offerings or this Agreement where a party seeks aggregate relief of $7,500 or more will be adjudicated in any state or federal court in King County, Washington. You consent to exclusive jurisdiction and venue in those courts.[125]

This contract essentially requires that any cloud computing dispute must be resolved in Washington State, even if the user is located in different part of the world.

---

[123] *See id.* ("There are occasions, particularly in the area of negligence, when the parties act without giving thought to the legal consequences of their conduct or to the law that may be applied. In such situations, the parties have no justified expectations to protect, and this factor can play no part in the decision of a choice-of-law question.").

[124] *See* Timothy J. Calloway, *Cloud Computing, Clickwrap Agreements, and Limitation on Liability Clauses: A Perfect Storm?*, 11 DUKE L. & TECH. REV. 163, 163 (discussing the negative effect that cloud provider clickwrap agreements could have on the cloud computing industry); *see, e.g.*, *Cloud Glossary*, EUCALYPTUS, http://www.eucalyptus.com/resources/ cloud-overview/cloud-glossary#q13 ("[A Service Level Agreement is a] contract, typically between a service provider and a service client, that stipulates the minimum quality of service the client will receive, the units and measurement methodology that will be used to audit service quality, and the time frame over which it will be measured."); *Sample Business Contract*, ONE CLE, http://contracts.onecle.com/gomez/ rackspace-services-2007-03-30.shtml. *See generally* Lynn Greiner & Lauren Gibbons Paul, *SLA Definitions and Solutions*, CIO, http://www.cio.com/article/128900/SLA_Definitions_and_Solutions.

[125] AWS CUSTOMER AGREEMENT, § 13.11, AMAZON WEB SERVICES, *available at* http://aws.amazon.com/agreement (last updated Aug. 23, 2011).

By analyzing the policies that affect cloud computing, one can see how critical location becomes in the legal context. Courts' own rules, which typically exercise jurisdiction through data center location, are often in direct contrast to choice-of-law provisions that govern in which state the issue must be litigated. Although courts respect choice-of-law provisions, lawyers can easily find loopholes in these contracts and bring suit in a location in which the data server sits.

D. International Provisions Regulating Data and Privacy

Conflict-of-law issues in the Internet context are aggravated by the fact that data is regulated differently throughout the world. If a corporation stores data in a cloud that has data servers in a foreign country, the law of that country may govern its data. Depending on the foreign country in which one's data is stored, the foreign country's law may affect 1) the privacy of your data and 2) whether that foreign country's government or police can access your data. In the European Union (EU), the laws on data privacy are highly developed and broad directives regulate data.[126] This is a result of the structure of the European political system and the view of privacy as a fundamental right, equal, if not superior, to economic rights.[127] In Asia, many countries have started to host data centers, but individual government attempts to regulate the industry are not as expansive as those in Europe.[128]

1. European Union Legislation Regulating Data

The European Commission, the executive body of the European Union ("EU"), represents the interests of the EU and

---

[126] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, arts. 2-4 1995 O.J. (L 281) 31, 31 (EC) [hereinafter Directive 95/46/EC].

[127] Eric Pfanner, *Guarding a "Fundamental Right" of Privacy in Europe*, N.Y. TIMES (Nov. 20, 2012), http://www.nytimes.com/2012/11/21/technology/guarding-a-fundamental-right-of-privacy-in-europe.html ("'In Europe, we consider privacy a fundamental right,' [French privacy regulator, Isabelle Falque-Pierrotin] said. 'That doesn't mean it is exclusive of other rights, but economic rights are not superior to privacy.'").

[128] *Compare infra* Part I.D.2 *with* Part I.D.1.

proposes legislation to the European Parliament and the European Council.[129] The European Commission is also responsible for administering and implementing EU policies and negotiating international matters.[130]

There are two major pieces of EU legislation that affect data: the Data Protection Directive 95/46/EC[131] and the proposed General Data Protection Regulation.[132] Since directives are the European form of legislation addressed to EU Member States,[133] each Member State is responsible for incorporating every directive into its own legal system, but the directive may still have legal force even if the member state has elected not enforced all of its provisions.[134]

Directive 95/46/EC of the European Parliament discusses the protection of individuals with respect to the processing of personal data.[135] The Directive's recitals generally "explain the background to the legislation and the aims and objectives of the legislation."[136] Recitals (6)–(8) and (20) specifically provide objectives for the cross-border flow of data,[137] while Recitals (42)–(44) govern the

---

[129] *About this Site*, EUROPEAN COMMISSION, http://ec.europa.eu/about_en.htm (last updated Nov. 16, 2012).

[130] *Id.*

[131] Directive 95/46/EC, *supra* note 126.

[132] *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)*, COM (2012) 11 final (Jan. 25, 2012) [hereinafter *General Data Protection Regulation*].

[133] DATA PROTECTION IN THE EUROPEAN UNION, EUROPA, at 4, *available at* http://ec.europa.eu/justice/policies/privacy/docs/guide/guide-ukingdom_en.pdf (last visited Mar. 7, 2013).

[134] *Id.*

[135] *See* Directive 95/46/EC, *supra* note 126. The Directive defines "personal data" as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." *Id.*

[136] *Guide to the Approximation of European Union Environmental Legislation: Annex I: How To Interpret EU Environmental Legislation*, EUROPEAN COMMISSION, http://ec.europa.eu/environment/archives/guide/annex1.htm (last updated March 2, 2012).

[137] Directive 95/46/EC, *supra* note 126, at 31–33.

conditions that allow the member states in the EU to restrict access to information.[138]

Further, the Directive addresses the free movement of personal data.[139] Recitals (56)–(58) require that, to transfer personal data to a third party country outside of the EU, the country must attain an "adequate level of protection."[140] Hence, the EU does not allow cloud computing data servers to be located outside of the EU unless the adequacy standards are met.[141] Although this Directive was enacted in 1995, it continues to help limit European data from third party access.

On January 25, 2012, the European Commission announced a proposal to create a General Data Protection Regulation (the "Data Protection Regulation").[142] The Data Protection Regulation will differ from past directives because it will be immediately applicable to all member states, and will impose fines if member states do not comply.[143] The regulation will affect data processors and cross-border data transfers.[144]

---

138 *Id*. at 35.

139 *Id*. at 31.

140 *Id*. at 36–37. Specifically, it states that "the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer," may only take place if the country has an "adequate level of protection. *Id*. at 38; *see also Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks*, EXPORT.GOV, http://export.gov/safeharbor/ (last updated Apr. 11, 2012).

141 *See Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (last updated Feb. 11, 2013). As of February 11, 2013, the Commission has recognized Andorra, Argentina, Australia, Canada, Switzerland, Faeroe Islands, Guernsey, State of Israel, Isle of Man, Jersey, the U.S. Department of Commerce's Safe Harbor Privacy Principles, and the transfer of Air Passenger Name Record to the United States' Bureau of Customs and Border Protection as providing adequate protection. *Id.*

142 *General Data Protection Regulation*, *supra* note 132.

143 Jane Finlayson-Brown, *How to Prepare for Proposed EU Data Protection Regulation*, COMPUTERWEEKLY.COM, http://www.computerweekly.com/opinion/Proposed-EU-Data-Protection-Regulation-what-should-companies-be-thinking-about (last visited March 17, 2013).

144 *Id*.

2. Asian Governments' Approach to Regulating Data

Asian countries that currently host data centers have taken different approaches to regulating cloud computing than the U.S. and the EU. Some Asian countries' laws permit government access to data within the data server that is sitting on its territory.[145] This policy creates legal privacy issues when third party contractors, such as Google or Amazon, have other countries' data stored in data servers within these countries.

In Japan, the Ministry of Internal Affairs and Communications (MIC) regulates the cloud computing industry.[146] The Global ICT Policy Division of the MIC created a strategy for promoting the cloud computing industry both within Japan, through the development of the Kasumigaseki Cloud and the Local Government Cloud,[147] and internationally, through the development of "new cloud solutions in cooperation with Asian countries."[148] In November 2011, the Japanese government stated that in the future, it plans to address the following international issues: "[j]urisdiction over databases stored in other countries (e.g. privacy protection act)," "[d]ispute settlement mechanism[s]," "[c]ountermeasures against 'harmful' information," "[the] [p]ossibility of government intervention with respect to private-sector data," and "[o]wnership of [intellectual property rights] regarding data stored on a cloud data center in other countries."[149]

India's approach to investments and regulations in cloud computing technology has been delayed due to government uncertainty over data security and privacy.[150] Despite the

---

[145] *See* Carol Ko, *Cloud Legal Issues III: Data Privacy Laws in Asia*, ASIA CLOUD FORUM, http://www.asiacloudforum.com/content/cloud-legal-issues-iii-data-privacy-laws-asia (last visited Mar. 17, 2013).

[146] *See* YUMIKO MYOKEN, CLOUD COMPUTING IN JAPAN 3 (2009), *available at* http://ukinjapan.fco.gov.uk/resources/en/pdf/5606907/5633632/cloud-computing-japan.

[147] Kazutaka Nakamizo, *Cloud Services in Japan*, MINISTRY OF INTERNAL AFFAIRS AND COMMUNICATIONS, JAPAN, 6 (2011), http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/presentation/pdf/111102_1.pdf.

[148] *Id*.

[149] *Id*. at 8.

[150] Rahul Sachitanand, *Indian CIOs' Cloud Concerns*, TIMES OF INDIA (Jan. 5, 2012, 12:31 PM), http://articles.timesofindia.indiatimes.com/2012-01-05/services-apps/30592821_1_cloud-server-data.

uncertainty, the government continues to allow companies to place their data servers within its borders.[151] India's Information Technology Act of 2000 governs the privacy rights accorded to data servers. Provision 69 reads:

> If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

This provision allows the government to intercept data located in data servers within its territory.

Independently, Asian countries are trying to determine how to attract private corporations to build technology and cloud computing entities in their respective countries, while at the same time trying to regulate the growing industry and determine how much access they are going to give local police to the data servers on their territory.

3. International Treaties that Affect Cloud Computing Technology

The Budapest Convention on Cybercrime was the first international treaty addressing Computer and Internet Crime.[152] When the U.S. Senate ratified the treaty in August 2006, then-Senate Majority Leader Bill Frist commented, "[w]hile balancing civil liberty and privacy concerns, this treaty encourages the sharing of critical electronic evidence among foreign countries so that law enforcement can more effectively investigate and combat these crimes."[153]

---

[151] *See id.*

[152] *See* Convention on Cybercrime, Nov. 23, 2001, C.E.T.S. No. 185, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[153] *US Ratifies Treaty On Cybercrime*, IOL NEWS (Aug. 5, 2006, 12:06 PM), http://www.iol.co.za/news/world/us-ratifies-treaty-on-cybercrime-1.288245.

Article 19 of the Budapest Convention, entitled "Search and seizure of stored computer data," requires each Party to the treaty to adopt legislation permitting its "competent authorities" to access data servers in its territories without permission of the owner of information, and clause 3 provides local authorities permission to seize, remove, or make copies of the computer data.[154] Article 22, which discusses jurisdiction, mandates that each Party establish jurisdiction over any computer-related offense, when the offense is either committed in its territory or by one of its nationals.[155] Further, jurisdiction over offenses committed in its territory cannot be waived.[156] If two or more Parties claim jurisdiction over any offense listed in the Convention, "the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution."[157]

The Council of Europe has attempted to review the decisions made during the Budapest Convention because of the widespread use of cloud computing and the urgent need for increased international co-operation.[158] The United States and the EU refuse to draft another treaty on cybercrime, despite international growth of cross-border cybercrime.[159]

At the Twelfth UN Congress on Crime Prevention and Criminal Justice in 2010, countries met to discuss prevention and response to Cybercrime.[160] The United States, the EU, and other governing bodies that supported the Budapest Convention rejected

---

154 Convention on Cybercrime, *supra* note 152, at art. 19.

155 *Id*. at art. 22(1).

156 *Id*. at art. 22(2) ("Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.").

157 *Id*. at art. 22(5).

158 *See UN Rejects International Cybercrime Treaty*, COMPUTERWEEKLY.COM (Apr. 20, 2010, 3:44 PM), http://www.computerweekly.com/news/1280092617/UN-rejects-international-cybercrime-treaty ("Cloud computing trends in particular have led the Council of Europe to open a review of the Budapest Convention.").

159 *Id*.

160 Twelfth United Nations Congress on Crime Prevention and Criminal Justice, Salvador, Braz., Apr. 12–19, 2010, *12th United Nations Congress on Crime Prevention and Criminal Justice Opens Today*, U.N. Doc. UNIS/CP/601 (Apr. 12, 2010), *available at* http://www.un.org/en/conf/crimecongress2010/pdf/pr100412-2.pdf.

Russia and China's proposal for a new Cybercrime treaty.[161] Both the United States and the EU asked for more stringent privacy protections in the Budapest Convention to protect against "over-zealous" police intervention into cloud computing data servers stored in other countries.[162]

II. LEGAL ANALYSIS

As demonstrated above, countries approach differently the question of how best to regulate the burgeoning cloud computing industry and whether there should be cross-country restrictions on data.[163] Scholars who have studied cloud computing, as well representatives of the cloud computing industry, are divided on how the government should regulate the industry in the future. As demonstrated in the introduction, the location of data has broad implications regarding who can access the data and which countries' laws regulate access to information. This Part first presents the tension between U.S. and EU policy and law regarding cloud computing, then explores competing legal theories on the future regulation of cloud computing technology.

A. The U.S. Government's Approach to Regulating Cloud Computing Technology

In the United States, privacy and technology law is sector-specific and is governed by a varying blend of legislation, regulation, and self-regulation.[164] As will be seen, this blended approach presents unique challenges as the United States seeks to strike the proper regulatory balance.

---

[161] *See Conflict Over Proposed United Nations Cybercrime Treaty*, COMPUTERWEEKLY.COM, (Apr. 15, 2010, 10:44 AM), http://www.computerweekly.com/news/1280092581/Conflict-over-proposed-United-Nations-cybercrime-treaty.

[162] *UN Rejects International Cybercrime Treaty*, *supra* note 158.

[163] *See* Patrick Baillie, *Can European Firms Legally Use U.S. Clouds To Store Data?*, FORBES (Jan. 2, 2012, 6:05 PM), http://www.forbes.com/sites/ciocentral/2012/01/02/can-european-firms-legally-use-u-s-clouds-to-store-data/ (describing the main differences between U.S. and EU law).

[164] *See U.S.-EU Safe Harbor Overview*, EXPORT.GOV, http://export.gov/safeharbor/eu/eg_main_018476.asp (last updated Apr. 26, 2012).

1. Governing Cloud Computing Through Legislation

Legislation governing cloud computing is tailored to the consumer and the industry. The data privacy rules of the Health Insurance Portability and Accountability Act (HIPAA), for example, are vastly different from those in the Gramm-Leach-Bliley Act (GLBA), which regulates the financial sector.[165] HIPAA places heavy restrictions on agreements with cloud service providers and mandates that parties enter into a business associate contract to protect private patient information.[166] The GLBA, in contrast, requires that financial institutions enter into strict contracts with service providers, prohibiting the service provider from disclosing user information except under specific circumstances.[167]

The U.S. Patriot Act, originally developed as a response to the September 11, 2001 terrorism acts, is one of the only laws that affects the entire cloud computing industry. Under the Act, a U.S.-based cloud service provider is subject to rules requiring it to turn over user information.[168] Section 217 states, "[i]t shall not be unlawful . . . for a person . . . to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer" if 1) the owner of the computer

---

[165] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1341 (1999) ("An Act [t]o enhance competition in the financial services industry by providing a prudential framework for the affiliation of banks, securities firms, insurance companies, and other financial service providers . . . .").

[166] *See, e.g.*, Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 264, 110 Stat. 1936; LISA J. SOTTO, BRIDGET C. TREACY & MELINDA L. MCLELLAN, PRIVACY AND DATA SECURITY RISKS IN CLOUD COMPUTING, 2–3 (2010).

[167] SOTTO, ET AL., *supra* note 166, at 2; *see Gramm-Leach-Bliley Act*, BUREAU OF CONSUMER PROTECTION BUSINESS CENTER, http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act (last visited Mar. 17, 2013).

[168] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, § 217, 115 Stat. 272 ("It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer . . . .") [hereinafter Patriot Act]; Sean Gallager, *PATRIOT Act and Privacy Laws Take a Bite Out of US Cloud Business*, ARS TECHNICA (Dec. 8, 2011, 8:49 AM), http://arstechnica.com/tech-policy/news/2011/12/patriot-act-and-privacy-laws-take-a-bite-out-of-us-cloud-business.ars (discussing Microsoft's inability to guarantee that its client's data wouldn't leave Europe).

authorizes the "interception of the computer trespasser's communications on the protected computer"; 2) the person is engaged in an investigation; 3) the person "has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation"; and 4) "such interception does not acquire communications other than those transmitted to or from the computer trespasser."[169]

Many members of government have recognized the sweeping effect of the U.S. Patriot Act. Steven M. Martinez, while Deputy Assistant Director of the FBI's Cyber Division, addressed the U.S. House of Representatives Subcommittee on Crime, Terrorism, and Homeland Security in Washington, D.C. on April 21, 2005.[170] He testified that:

> Section 220 [of the Patriot Act] enables federal courts—with jurisdiction over an investigation—to issue a search warrant to compel the production of information (such as unopened e-mail) that is stored with a service provider located outside their district. The practical effect of this section is that our FBI Agents are no longer limited to applying for a search warrant solely from the court that sits where the service provider happens to be located.[171]

Section 220 broadly expands the power of the government to access information stored within data servers on U.S. soil as well as internationally.

Private corporations are required to comply with the Patriot Act.[172] According to a *Forbes* article in January 2012, "[b]oth Amazon Web Services and Microsoft have recently acknowledged that they would comply with U.S. government requests to release data stored in their European clouds, even though those clouds are located outside of direct U.S. jurisdiction and would conflict with

---

169 Patriot Act, *supra* note 168.

170 Steven M. Martinez, Deputy Assistant Director, Cyber Division, Federal Bureau of Investigation, Testimony at the Subcommittee on Crime, Terrorism, and Homeland Security (Apr. 21, 2005), *available at* http://www.fbi.gov/news/testimony/computer-provisions-of-the-usa-patriot-act.

171 *Id.*

172 *See* Patriot Act, *supra* note 168, at § 1016.

European laws."[173] The strict requirements of the Patriot Act have caused several countries overseas to enact laws that restrict electronic data flow within their borders.[174] By restricting data flow to servers within their borders, the United States could not obtain proper jurisdiction to access their information.

2. Governing Cloud Computing Through Regulation

United States government agencies are attempting to self-regulate their IT practices, including the circumstances under which cloud computing can operate and serve as a tool to the government, while also complying with the Cloud First Policy. The U.S. agencies involved in export controls, or the trans-border restriction of data, have led the self-regulation movement in the cloud computing context.[175] The Departments of State, the Treasury, Energy, Defense, and the Interior, the Nuclear Regulatory Commission, the Environmental Protection Agency, the Food and Drug Administration, and other government organizations all govern export controls.[176]

The National Institute of Standards and Technology (NIST) is the agency within the Department of Commerce that assists in regulating the technology industry.[177] The Information Technology Laboratory (ITL) is a branch of NIST tasked with promoting "U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology."[178] The ITL has released for public comment two proposed roadmaps that "define[] high-priority requirements for standards, official guidance and technology developments that need to be met in order for agencies to accelerate their migration of existing IT

---

173 Baillie, *supra* note 163.

174 *See, e.g.*, David Saleh Rauf, *PATRIOT Act Clouds Picture for Tech*, POLITICO (Nov. 29, 2011, 11:17 PM), http://www.politico.com/news/stories/1111/69366_Page2.html.

175 *See* VILLASENOR, *supra* note 26, at 1–2.

176 *United States Government Departments and Agencies with Export Control Responsibilities*, BUREAU OF INDUSTRY & SECURITY, U.S. DEP'T OF COMMERCE, http://www.bis.doc.gov/about/reslinks.htm (last visited Mar. 17, 2013).

177 *About NIST*, NIST (Aug. 18, 2009), http://www.nist.gov/public_affairs/nandyou.cfm (last updated Apr. 18, 2012).

178 *What ITL Does*, NIST (Jan. 7, 2010), http://www.nist.gov/itl/what-itl-does.cfm (last updated Jan. 25, 2011).

systems to the cloud computing model."[179] While the roadmaps discuss security requirements, there are no substantive rules that regulate where data can be stored or how data can pass between borders.

The General Services Administration ("GSA") is the Federal Agency that oversees the business side of the federal government.[180] Part of the responsibility of the GSA includes managing federal buildings, building public trust in the government, as well as selecting "high-quality, low-cost goods and services" available for purchase by the federal government's agencies and employees.[181] When the GSA received $2.5 billion in 2011 to spend on cloud e-mail services for federal employees, private technology companies tried to contract with the GSA to provide these services.[182]

In October 2011, two contracting firms that provide cloud computing services, Technosource Information Systems and TrueTandem, filed protests with the Government Accountability Office ("GAO") over the fact that the GSA required all data centers to either be located in the United States,[183] or in designated countries as defined by Federal Acquisition Regulation ("FAR")

---

[179] *Draft Roadmap for Cloud Computing Technology*, NIST (Nov. 8, 2011), http://www.nist.gov/itl/cloud-110811.cfm.

[180] *Background and History*, U.S. GEN. SERVS. ADMIN., http://www.gsa.gov/portal/content/ 104774 (last updated Feb. 14, 2013).

[181] *A Brief History of GSA*, U.S. GEN. SERVS. ADMIN., http://www.gsa.gov/portal/content/103369 (last updated Feb. 25, 2013).

[182] *See* Alice Lipowicz, *GSA Launches $2.5B Cloud Computing Procurement*, WASHINGTON TECHNOLOGY (May 10, 2011), http://washingtontechnology.com/articles/2011/05/10/gsa-issues-rfq-for-cloud-computing-options.aspx; Ed O'Keefe & Majorie Censer, *Contract With Ties to Microsoft and Google Needs Change, GAO Says*, WASH. POST (Oct. 17, 2011, 3:10 PM), http://www.washingtonpost.com/politics/contract-with-ties-to-microsoft-and-google-needs-changes-gao-says/2011/10/17/gIQAPktPsL_story.html.

[183] *See* Technosource Info. Servs., LLC, B-405296 *et al*., Comp. Gen. (2011), *available at* http://www.gao.gov/decisions/bidpro/405296.pdf ("Technosource Information Systems, LLC, or Annapolis, Maryland, and TrueTandem, LLC, of Reston, Virginia, protest the terms of request for quotations . . . issued by the General Services Administration . . . for cloud computing services.").

section 25.003.[184] Essentially, this requirement allowed data centers to be placed in war-torn "countries including Afghanistan, Yemen, and Somalia . . . but not in countries with developing tech sectors" such as India.[185] The GSA argued that the government must know where its data is stored, "because when U.S. government data crosses national borders, the governing legal, privacy, and regulatory regimes become ambiguous and raise a variety of concerns including the potential of foreign jurisdictions to assert access rights to U.S. government data."[186]

The GAO then held a hearing on this matter and asked the GSA to explain its data center requirement.[187] The GSA explained that it had originally limited the location of data servers to the United States, but compromised because the Office of Management and Budget (the "OMB") and the Office of the United States Trade Representative (the "USTR") advised the GSA that the requirement would have "impermissibly restricted free trade."[188] The contracting officer of the GSA admitted that the agency did not have a list of countries it considered acceptable, so the GSA limited the data centers to designated countries.[189]

The GAO concluded that the GSA requirements were "established in an arbitrary manner" as the GSA acknowledged it had "no basis to differentiate between countries with acceptable data rights regulations and those with unacceptable data rights regulations."[190] Additionally, the GAO found that "with regard to GSA's argument that the government has a need to know where U.S. government data resides and transits, this objective is accomplished by the requirement for vendors to identify the locations of their data centers."[191] The GAO sustained the

---

184 *See id.* at 2 n.1 ("FAR § 25.003 defines 'designated country' to include a World Trade Organization Government Procurement Agreement country, a Free Trade Agreement country, a least developed country, or a Caribbean Basin country.").

185 O'Keefe & Censer, *supra* note 182.

186 *Technosource*, *supra* note 183.

187 *Id.*

188 *Id.*

189 *Id.*

190 *Id.*

191 *Id.*

protesters' challenges, and recommended that the GSA amend the terms of its contract requirements.[192]

In November 2011, the GSA again solicited bids for Email-as-a-Service ("EaaS") government contracts.[193] This time the GSA did not impose any location requirements and simply asked the cloud computing service providers to identify where their data centers are located.[194]

As of January 2013, GSA contracts are still subject to the Trade Agreements Act, which requires that products "be manufactured or 'substantially transformed' in a 'designated country.'"[195] The designated country list, compiled by the Department of State, allows data centers to be located even in countries the government discourages Americans from traveling to, such as Afghanistan, Burundi, Eritrea, Guinea, Honduras, Mauritania, and Mexico.[196]

In November 2011, the U.S. Department of the Interior publicly issued a request for information to identify cloud service providers that are interested in providing cloud-based e-mail and collaboration services for the Department.[197] The request expressed the Department's preference that service providers keep their data centers located in the United States.[198]

---

[192] *See id*.

[193] *Email as a Service (EaaS)*, U.S. GENERAL SERVICES ADMINISTRATION, http://www.gsa.gov/portal/content/112223; Nick Wakeman, *GSA Restarts $2.5B E-Mail Contract*, WASHINGTON TECHNOLOGY (Nov. 30, 2011), http://washingtontechnology.com/articles/2011/11/30/gsa-cloud-email-rfq.aspx.

[194] TOM KIREILIS & GREG NORMAN, EMAIL AS A SERVICE (EAAS) BLANKET PURCHASE AGREEMENT (BPA) REQUIREMENTS DOCUMENT 4, *available at* http://gsa.gov/portal/getMediaData?mediaId=148887.

[195] *TAA Designated Countries*, FEDERAL SCHEDULES, INC., http://gsa.federalschedules.com/resource-center/resources/taa-designated-countries.aspx (last updated Feb. 2013).

[196] *Current Travel Warnings*, TRAVEL.STATE.GOV, http://travel.state.gov/travel/cis_pa_tw/tw/tw_1764.html (last visited Apr. 5, 2013).

[197] *Cloud E-Mail and Collaboration Services (CECS)—Request for Information, Capabilities, and Sources Sought*, FEDBIZOPPS.GOV (Oct. 28, 2011), https://fbo.gov/index?s=opportunity&mode=form&id=1ebb0fdd2b3c0be3c3ac38872f669d5b&tab=core&_cview=0.

[198] THE DEPARTMENT OF THE INTERIOR, CLOUD-BASED EMAIL AND COLLABORATION SERVICES (CECS) STATEMENT OF WORK 22 (2011) ("The physical data centers for this requirement must be located within the continental United States.").

In the United States, regulations governing cloud computing vary across agency. Some agencies, such as the Department of Commerce, are primarily concerned with a data server's security requirements, while other agencies, such as the GSA and the Department of the Interior, have raised concerns about the location of data servers, but have yet to create regulations.[199]

B. The EU's Hard Line Approach to Regulating Cloud Computing Conflicts with the United States' Laissez-faire Approach

The EU's Data Protection Directive 95/46/EC places strict standards on governments that collect electronic data.[200] Cloud computing data that originates from the European Economic Area (EEA) cannot be transferred to another country unless there is an adequate level of data protection.[201] The EU will find that a country does not have an adequate level of protection if it determines that the laws in the country in question, including professional rules and security measures, do not adequately protect data transfers.[202] The United States is not one of the countries that has a sufficient level of protection because of its weak data protection and inconsistent data regulation.[203]

Countries that want to work with the EEA can develop alternative legal options to meet the adequate level of protection

---

[199] *See infra* part II.B.2.

[200] William R. Denny, *Survey of Recent Developments in the Law of Cloud Computing and Software as a Service Agreement*, 66 BUS. LAW. 237, 239 (2010).

[201] SOTTO, *supra* note 166, at 4.

[202] Directive 95/46/EC, *supra* note 127, at 45–46 ("The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstance surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.").

[203] *See Sending Personal Data Outside the European Economic Area (Principle 8)*, INFORMATION COMMISSIONER'S OFFICE, http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_8.aspx (last visited Mar. 18, 2013). Despite not being on the list of approved countries, the U.S. can still be sent personal data if "a US company signs up to the Safe Harbor arrangement [and] agree[s] to: following seven principles of information handling; and be held responsible for keeping to those principles by the Federal Trade Commission or other oversight schemes." *Id.*

standard.[204] For example, the U.S. Department of Commerce's Safe Harbor Program purports to align the strict EU Data Protection Directive 95/46/EC with U.S. data privacy controls.[205] Its goal is to provide a simpler mechanism for U.S. organizations to comply with the EU directive, without U.S. organizations having to follow each of the EU's requirements.[206]

There are seven main Safe Harbor privacy requirements with which an organization must comply to meet EU adequacy standards.[207] These include 1) Notice ("organizations must notify individuals about the purposes for which they collect and use information about them" and the types of third parties this information is disclosed to); 2) Choice (organizations "must give individuals the opportunity to choose" whether their information will be disclosed to a third party or used for a purpose other than the one the individuals agreed to); 3) Onward Transfer (to disclose information to a third party, organizations must give notice and choice); 4) Access ("individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate" except where the burden of access is disproportionate to risks of the individual's privacy); 5) Security (organizations must protect personal information from "loss, misuse and unauthorized access, disclosure, alteration and destruction"); 6) Data Integrity ("[p]ersonal information must be relevant for the purposes for which it is to be used"); and 7) Enforcement (there must be available and independent recourse mechanisms so each individual's complaints can be investigated and resolved, procedures for verifying that companies that adhere to safe harbor principles obligations to remedy problems of failure to comply, and sanctions for non-compliance).[208] The Department of Commerce proclaimed that government agencies, the Federal

---

[204] *See, e.g.*, *id.* ("The Safe Harbor scheme is recognised by the European Commission as providing adequate protection for the rights of data individuals in connection the [sic] transfer of their personal data to signatories of the scheme in the USA.").

[205] *U.S.-EU Safe Harbor Overview*, EXPORT.GOV, http://export.gov/safeharbor/eu/eg_main_018476.asp (last updated Apr. 26, 2012).

[206] *See id.* ("Compliance requirements are streamlined and cost-effective . . . .").

[207] *Id.*

[208] *Id.*

Trade Commission, and state governments may force corporations to comply with the Safe Harbor Privacy Principles at any time.[209]

Another way that countries work with the strict EU requirements is to restrict data flow within a country's borders. Some international cloud service providers have special EU-only data clouds that prevent EU data from being transferring outside of the EU.[210] Under EU data law, individuals have a fundamental right to delete or access their personal data.[211] This requires cloud service providers to communicate effectively with individuals and indicate where their data is stored.[212]

C. Proposals Moving Forward

Industry groups, academic scholars, and cloud service providers in the United States are divided on how cloud computing should be regulated.

1. Industry-Led Self-Regulation for Cloud Computing

The Software and Information Industry Association (the "SIIA") and Cloud Security Alliance are the largest groups advocating minimal regulation of the cloud computing space. The SIIA comprises 500 software and information companies.[213] The position of SIIA is that the cloud computing industry should self-regulate, and the government should not create laws for the industry to follow.[214] The SIIA wants to "[p]romote open

---

[209] *See id*. ("Depending on the industry sector, the Federal Trade Commission, comparable U.S. government agencies, and/or states may provide overarching government enforcement of the Safe Harbor Privacy Principles.").

[210] SOTTO, *supra* note 166, at 4.

[211] *Id*. at 5.

[212] *See id*.; *Opinion 05/2012 on Cloud Computing*, at 11, WP 196 (July 1, 2012) (stating that transparency requires providers to inform individuals of all subcontractors "contributing to the provision of the respective cloud service" as well as the location of all data centers where personal data is processed).

[213] Hayley Tsukayama, *No Need for Cloud-Specific Legislation, SIIA Industry Group Says*, The WASH. POST (JULY 26, 2011, 9:04 AM), http://www.washingtonpost.com/blogs/post-tech/post/no-need-for-cloud-specific-legislation-siia-industry-group-says/2011/07/26/gIQAHaEaaI_blog.html.

[214] *See SIIA's Cloud Computing Recommendations for Policymakers*, SOFTWARE & INFORMATION INDUSTRY ASSOCIATION, http://www.siia.net/index.php?option=com_

standards for software and data interoperability, and avoid policies that would favor one particular business model or technology over another . . . [and] [p]romote policies that allow to the greatest extent possible, unrestricted transfer of data across borders."[215]

The SIIA works with the U.S. government, particularly the National Institute of Standards and Technology, to create open standards for privacy and data security under the current "Cloud First" policy.[216] The Cloud Security Alliance is a group of industry practitioners and corporations that work to promote the use of best practices for addressing security issues when using cloud computing technology.[217] The Cloud Security Alliance advocates minimal government intrusion.[218] Both the CSA and the SIIA believe that if one country's regulations are too restrictive on the movement of data and privacy, cloud service providers should simply move their data to a different location.

2. Cloud Computing Needs Regulation and Clarity

Academic scholars have set forth the view that cloud computing regulations are essential to U.S. national security and foreign policy interests.[219] However, scholars taking this stance dispute whether cloud computing should be regulated through the manipulation of export controls or through jurisdiction and contractual obligations.[220] These scholars are concerned that flexibility in cloud computing is not worth the uncertainty of the

content&view=article&id=807:siias-cloud-computing-recommendations-for-policymakers&catid=163:public-policy-articles (last visited Mar. 29, 2013).

[215] *Id*.

[216] *See* Letter from Ken Wasch, President, Software & Info. Indus. Ass'n, to Dawn Leaf, Exec. Program Manager, Cloud Computing, Nat'l Inst. of Standards and Tech. (Dec. 13, 2011), *available at* http://siia.net/index.php?option=com_docman&task=doc_download&gid=3235&Itemid=318.

[217] *About*, CLOUD SECURITY ALLIANCE, https://cloudsecurityalliance.org/about (last visited Mar. 19, 2013).

[218] *See STAR FAQ*, CLOUD SECURITY ALLIANCE, https://cloudsecurityalliance.org/star/faq (last visited Mar. 19, 2013) ("In these early days of cloud adoption, voluntary self-regulation of cloud providers is preferable to heavy handed governmental regulation.").

[219] *See generally* Villasenor, *supra* note 26, at 1 (discussing why cloud computing should be regulated).

[220] *See id*. at 1–2 (discussing how issues of jurisdiction related to cloud control have been studied, but not enough attention has been given to export control and its relationship to cloud computing).

location of data in the cloud or the vague contractual terms, unless there are strict regulations controlling jurisdiction and contractual obligations.[221] They consider cloud computing an "immature and rapidly-developing market" where there is a "mismatch" between consumer expectations and the services consumers receive.[222] Issues with the location of data may create conflicts if the contract specifies a foreign legal system and jurisdiction.[223]

The Brookings Institute, a nonprofit public research and policy organization in Washington, D.C., champions the regulation of cloud computing.[224] Its Board of Trustees is comprised of distinguished representatives from a broad swath of the public, including the Chief Investment Officer of Yale University.[225] The Brookings Institute argues that if no action is taken to regulate cloud computing, the government's failure to regulate may weaken the entire U.S. export control system.[226]

John Villasenor, senior fellow in Governance Studies at the Center for Technology Innovation at Brookings, favors regulation in security, privacy and jurisdictional issues.[227] Villasenor recommends that cloud service providers give users a choice over the location of the server storing their data.[228] Under this plan, users would be able to choose if they want to pay "a slight premium to ensure the assignment of servers based in the United

---

221 *See* Simon Bradshaw, Christopher Millard, & Ian Walden, *The Terms They Are A-Changin' . . . Watching Cloud Contracts Take Shape*, 7 ISSUES IN TECH. INNOVATION 1, 1, 5–6 (2011), *available at* http://www.brookings.edu/papers/2011/03_cloud_computing_contracts.aspx.

222 *Id*. at 11.

223 *Id*. at 2.

224 The goals of the Institute are to "[s]trengthen American democracy . . . .[f]oster the economic and social welfare, security and opportunity of all Americans[and] . . . "[s]ecure a more open, safe, prosperous and cooperative international system." *About Brookings*, BROOKINGS INST., http://www.brookings.edu/about.aspx (last visited Mar. 19, 2013).

225 *See Board of Trustees*, BROOKINGS INST., http://www.brookings.edu/about/Trustees.aspx (last visited Mar. 19, 2012); ("The Brookings Board of Trustees is composed of distinguished business executives, academics, former government officials and community leaders.").

226 *See* VILLASENOR, *supra* note 26, at 10.

227 *See id*.

228 *See id*. at 7.

States," and thus have a more secured server.[229] A pricing plan may set off the cost to cloud computing technology companies.[230]

3. Cloud Computing Service Providers Attempt to Control Which Law Governs Their Data Servers

The Cloud Legal Project at the Centre for Commercial Law Studies, based at the School of Law at Queen Mary, University of London, conducted a survey of thirty-one cloud computing contracts from twenty-seven different providers.[231] The study found that these contracts mandate that law from various U.S. states or English law applied and could force users to defend a suit in an unfamiliar place.[232] Some countries outside the United States do not have the same civil rights safeguards.[233] Without legislation and policy, users of cloud computing services could be subject to arbitrary laws.[234]

The surveyed contracts often had exclusion clauses and disclaimers buried deep within the contract terms that allow the companies to alter these contracts at will.[235] For instance, the Amazon Web Service Customer Agreement (2011) states, "[w]e may modify this Agreement (including any Policies) at any time by posting a revised version on the AWS Site . . . . By continuing to use the Service Offerings after the effective date of any modifications to this Agreement, you agree to be bound by the modified terms."[236] Here, Amazon essentially reserves the right to

---

229 *Id*.

230 *See id*. at 7–8.

231 *See* Simon Bradshaw, Christopher Millard, & Ian Walden, *Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*, 19 INT'L J. L. & INFO. TECH. 187, 191 (2011). The survey included the following providers: 37signals, 3tera, Adrive, Akamai, Amazon, Apple, Decho, Dropbox, ElasticHosts, Facebook, Flexiant, G.ho.st, GoGrid, Google, IBM, Iron Mountain, Joyent, Microsoft, Nirvanix, PayPal, Rackspace UK, Salesforce, Symantec, The Planet, UKFast, Zecter, and Zoho. *Id*. at 193–94. The survey was partially funded by Microsoft. *Id*. at 187 n.*.

232 *Id*. at 198–200.

233 Jaeger, *supra* note 15, at § 5.

234 *See id*.

235 Bradshaw, *supra* note 231, at 9 ("A large portion of the contracts we analyzed included terms providing that the provider could amend the contract simply by posting an updated version on its web site; if a customer continues to use the service, this is deemed acceptance of the new terms.").

236 AWS CUSTOMER AGREEMENT, *supra* note 125, at § 12.

modify its contract, or the terms governing the location of its data servers.

These technology companies often have terms of service that limit liability of the company.[237] Terms in Google's "Google Apps for Business Online Agreement" govern requests by third parties to access private information:[238]

> Customer is responsible for responding to Third Party Requests. Google will, to the extent allowed by law and by the terms of the Third Party Request: (a) promptly notify Customer of its receipt of a Third Party Request; (b) comply with Customer's reasonable requests regarding its efforts to oppose a Third Party Request; and (c) provide Customer with the information or tools required for Customer to respond to the Third Party Request. Customer will first seek to obtain the information required to respond to the Third Party Request on its own, and will contact Google only if it cannot reasonably obtain such information.[239]

It is unclear if this provision applies to "Google Apps for Government." These customer agreements often have vague terms because the service providers may not know which country's law governs their contracts and whether police enforcement could access confidential user data.[240]

Public and private companies that provide cloud computing services are often unaware of the laws that apply to their data

---

[237] *See, e.g.*, *AWS Service Terms*, AMAZON WEB SERVICES, http://aws.amazon.com/serviceterms/ (last updated Mar. 7, 2013) ("We have no liability or responsibility with respect to any delay, damage or loss incurred during shipment, including loss of Data."); *Google Apps for Business (Online) Agreement*, GOOGLE APPS, http://www.google.com/apps/intl/en/terms/premier_terms.html (last updated Mar. 28, 2012) ("Neither party will be liable under this agreement for lost revenues or indirect, special, incidental, consequential, exemplary, or punitive damages, even if the party knew or should have known that such damages were possible and even if direct damages do not satisfy a remedy.").

[238] *See Google Apps for Business (Online) Agreement*, supra note 237.

[239] *Id.*

[240] *See* BRAD SMITH, BUILDING CONFIDENCE IN THE CLOUD: A PROPOSAL FOR INDUSTRY AND GOVERNMENT ACTION TO ADVANCE CLOUD COMPUTING 7.

servers or the information they contain. A Microsoft memo on building the cloud industry observed,

> There are, however, no universally agreed upon rules governing such access by law enforcement. The result is that service providers are increasingly subject to divergent, and at times conflicting, rules governing jurisdiction over user content and data. Further complicating the problem is the fact that different jurisdictions also have different laws regarding privacy rights and data retention.[241]

These conflicting messages make it difficult for cloud service providers to meet consumer expectations for competent privacy and security protections.[242]

D. Potential Conflicts if the Government Does Establish Uniform Regulation

There are many loopholes in the U.S. government's approach to regulating cloud computing technology. The GAO has identified a number of negative security implications that would occur if the government continues to neglect regulation of the cloud computing industry.[243] Twenty-two of twenty-four major federal agencies reported that they were "concerned or very concerned about the potential information security risks associated with cloud computing."[244]

If sensitive U.S. government data is sitting in countries that abide by the Budapest Convention on Cybercrime, local police may have access to private government information.[245] Access

---

241 *Id*.

242 *Id*. ("This global thicket of competing and conflicting laws presents a significant obstacle to the delivery of cloud services that meet users' reasonable expectations of privacy.").

243 *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-130T, Information Security: Additional Guidance Needed to Address Cloud Computing Concerns 6–7 (2011), *available at* http://www.gao.gov/products/GAO-12-130T ("The use of cloud computing can also create numerous information security risks for federal agencies. . . . Several of these risks relate to being dependent on a vendor's security assurances and practices.").

244 *Id*. at 6.

245 *See* Convention on Cybercrime, *supra* note 152, at art. 19(1) ("Each Party shall adopt such legislative and other measures as may be necessary to empower its competent

may be necessary in certain emergency situations such a data server meltdown, but the Budapest Convention mandates a low standard for abridging private rights.[246]

Another potential problem is that government contracts with private companies often do not include terms dictating the location of the data servers that hold their information. With choice of law provisions unclear as to whether a data server implicates a legal interest, it is difficult to determine what law would apply overseas in a security breach of a server. Contractual provisions could solve this problem, but private companies currently have full discretion to change their terms at any point.[247]

III. RECOMMENDATIONS

The federal government must have absolute control over the storage of its electronic information, including the ability to select safe countries to host this information and the right to determine the frequency with which private and public data service providers can move the government's information to different servers.

A. Cloud Computing Regulations Will Secure Government Information

Some scholars have found that the main reason for the lack of cloud computing regulations in the United States is a "lack of a political infrastructure that reacts deftly to rapid technological

authorities to search or similarly access: (a) a computer or part of it and computer data stored therein; and (b) a computer-data storage medium in which computer data may be stored, in its territory.").

246 *See id.* at art. 19(2) ("Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or party of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.").

247 Bradshaw, *supra* note 231, at 9 ("A large portion of the contracts we analyzed included terms providing that the provider could amend the contract simply by posting an updated version on its web site; if a customer continues to use the service, this is deemed acceptance of the new terms.").

change."[248] The transmission of sensitive government information to data servers around the world creates an urgent need for broad directives to protect our private information from unwarranted intrusions. In a cloud computing environment, the owner of data loses control to a third party company that chooses the storage location of the owner's data.[249] The United States needs regulations, similar to EU data directives, to protect private government information. When data is stored in other countries, these types of regulations are vital in preventing other countries from conducting arbitrary server inspections or claiming a right to access to the actual data stored on each server.

With increasing frequency, private companies that offer cloud computing services are reporting breaches of security. It is estimated that U.S. businesses and institutions lose sixty-seven billion dollars to cybercrime every year.[250] Microsoft has admitted that, "the aggregation of massive amounts of data in large datacenters also creates a new and highly tempting target for criminals. As criminals turn their attention to these vaults of information . . . it will become increasingly challenging to protect such datacenters from both physical and cyber attacks."[251] The prospect of attacks on the countries—as well as the physical location of data servers—makes information protection a major concern.

The U.S. government must act to prevent foreign countries accessing data servers sitting on their territories from circumventing U.S. law.[252]

---

248 Jaeger et al., *supra* note 15, at § 6.

249 Irion, *supra* note 79, at 9.

250 Twelfth United Nations Congress on Crime Prevention and Criminal Justice, Salvador, Braz., Apr. 12–19, 2010, *Recent Developments in the Use of Science and Technology by Offenders and by Competent Authorities in Fighting Crime, Including the Case of Cybercrime*, ¶ 8, U.N. Doc. A/CONF.213/9 (Jan. 22, 2010), *available at* http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050382e.pdf.

251 SMITH, *supra* note 240, at 2.

252 *See id.* ("For the cloud to deliver on its promise, Congress needs to take responsible action to foster users' confidence that their privacy interests will be preserved and their data will remain secure in the cloud.").

B. One Way to Ensure the Security of Government Information is for the Government to Purchase its own Private Data Centers

The U.S. government should explore the option of building its own private data servers on U.S. soil. As the government has saved significant capital storing its data on server farms, some of these reserves should be used towards securing this information. One way to ensure that one's property is completely secure is to safeguard that property oneself. If it were not for the digitization of data, the U.S. Government would never think to outsource the storage of hard copy files.

To obtain this high level of security, the government should build its own private data centers. The government is currently the largest property owner in the U.S., holding 1.2 million individual properties.[253] Much of this property is either empty or underutilized, and the Obama Administration categorizes this property as "excess."[254] These excess properties cost American taxpayers an estimated "$190 million a year."[255] Although it would be costly to develop the software infrastructure needed, the government could contract out services to technology companies, but require that the information is stored on its property.

C. If it is Not Feasible for the Government to Own its Own Data Centers, Data Servers Containing Private Government Information Should Remain in the United States

If it is not feasible for the government to build its own data servers because the program would be too costly or time consuming, the government should mandate that data centers storing its information remain in the U.S.

U.S. cities have lead this initiative. For example, the City of Los Angeles ("LA") contracts out e-mail service and data storage

---

253 *Cutting Costs by Getting Rid of Buildings We Don't Need*, THE WHITE HOUSE, http://www.whitehouse.gov/issues/fiscal/excess-property-map (last visited Mar. 20, 2013); Jared A. Favole, *Uncle Sam Finds 14,000 Facilities to Sell*, WALL ST. J. (Mar. 2, 2011, 7:36 PM), http://blogs.wsj.com/washwire/2011/03/02/uncle-sam-finds-14000-facilities-to-sell.

254 *See id.*

255 *Id.*

to Google.[256] In LA's contract with Google, LA requires that e-mail data be stored and processed only in data servers in the continental U.S.[257] However, Google does not have enough data server capacity in the U.S. to store both e-mail and other data.[258] LA requires notice from Google when space in Google's U.S. data server's becomes available, so LA can migrate non-e-mail data to Google's U.S. servers.[259] While most LA city employees use Gmail for e-mail, the LAPD cannot use Google services because the data servers that run Google Apps for Government are located in the EU.[260] Google cannot require EU employees, who run Google's international data servers, to submit to background checks to meet the standards of the LAPD.[261] If the U.S. government were to stand behind LA's decision, cloud computing service providers would have to create more secure U.S.-based data servers.

---

[256] *See* David Sarno, *L.A. Won't Put LAPD on Google's Cloud-Based Email System*, L.A. Times (Dec. 14, 2011), http://articles.latimes.com/2011/dec/14/business/la-fi-google-email-20111215.

[257] Contract Number C-116359, Between the City of Los Angeles and Computer Science Corporation for the SaaS E-Mail and Collaboration Solution (SECS) § 1.7 (Nov. 10, 2009), *available at* http://clkrep.lacity.org/onlinecontracts/2009/C-116359_c_11-20-09.pdf, Appendix J.1, Section 1.7 of the Professional Services Contract between Google and the City of Los Angeles ("Google agrees to store and process Customer's email and Google Message Discovery (GMD) data only in the continental United States. As soon as it shall become commercially feasible, Google shall store and process all other Customer Data, from any other Google Apps applications, only in the continental United States. Google shall make commercially reasonable efforts to advise Customer when such data storage capability is made available. Notwithstanding the foregoing, Google may store and process Login Data in any country in which Google or its agents maintain facilities.").

[258] *See* Sarno, *supra* note 256 ("Google may have overestimated its ability to satisfy strict federal security rules about sensitive data from law enforcement agencies. . . . [T]he rules were written for law enforcement agencies that store their own data and did not consider the increasingly popular cloud computing model.").

[259] Contract Number C-116359, *supra* note 257, at § 1.7.

[260] *See* Jeff Gould, *Los Angeles Pulling the Plug on Gmail at LAPD is Much Bigger than You Think*, SAFEGOV (Dec. 15, 2011), http://safegov.org/2011/12/15/los-angeles-pulling-the-plug-on-gmail-at-lapd-is-much-bigger-than-you-think ("[A]nalyst firm Gartner reported in July that some of Google's support staff with access to [Google Apps for Government] servers are based on Europe.");

[261] *See id.* ("The FBI doesn't explicitly mandate that support personnel be located in the U.S., but European law may make it difficult for Google to force its European employees to submit to screening (including fingerprinting) by U.S. authorities.").

It is also important that the U.S. government move away from the idea that cloud computing regulations "restrict free trade."[262] The OMB and the USTR must recognize that these regulations are in place to secure private government and consumer data. As discussed earlier, many countries around the world restrict the flow of data to within their borders; there is no reason the United States should not also adopt this policy.

In addition to the proposition that government information must remain in the U.S., broad regulations governing contracts with private parties are necessary to achieve security through the cloud computing agenda. NIST is one of the only agencies that has comprehensively thought about the different requirements for the various cloud computing platforms.[263] NIST has also considered the interdependency of the U.S. government's cloud computing program with other cyber security and national security initiatives.[264] The problem is that NIST lacks the authority to regulate other government agencies and only has the authority to create a roadmap or guidance document.[265] It is important that Congress delegate the authority to develop a plan to protect government information.

The uncoordinated U.S. approach contrasts starkly with the pool of countries that *have* developed comprehensive cloud computing laws. The United States is supposed to be a global technology leader, but among most developed countries, the

---

[262] Technosource Info. Servs., LLC, B-405296 *et al*., Comp. Gen. (2011), *available at* http://www.gao.gov/decisions/bidpro/405296.pdf.

[263] *See* PETER MELL & TIMOTHY GRANCE, THE NIST DEFINITION OF CLOUD COMPUTING: RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 1 (2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf ("The intended audience of this document is system planners, program managers, technologists, and others adopting cloud computing as consumers or providers of cloud services.").

[264] LEE BADGER, TIM GRANCE, ROBERT PATT-CORNER, & JEFF VOAS, CLOUD COMPUTING SYNOPSIS AND RECOMMENDATIONS ES-2, 1-1 (2012), *available at* http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf.

[265] *Id*. at 1-1 ("Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority, nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official.").

United States has the least cohesive security plans regulating cloud computing technology.

CONCLUSION

No government agency has comprehensively looked at all of the risks concerning cloud computing technology, and the law of countries where data servers are located. As the government increasingly moves sensitive data to private companies that are free to store information in massive data servers overseas, U.S. citizens face countless threats to their privacy and the security of their data. The government must at least attempt to keep its own information on U.S. soil. If this is not feasible, data servers containing sensitive government information must at least remain in the United States.