Center for Technology Innovation at BROOKINGS

July 25, 2011

Reuters/Valentin Flaraud – A technician performs maintenance in the CERN LHC computing grid centre in Geneva

Addressing Export Control in the Age of Cloud Computing

John Villasenor

EXECUTIVE SUMMARY

The move to the cloud is one of the defining information technology trends of the early 21st century. By providing businesses, universities, government agencies, and other entities with access to shared and often physically dispersed computing resources, cloud computing can simultaneously offer increased flexibility, reduced cost, and access to a wider array of services.

Cloud computing has also created a set of new challenges. For example, the issues of privacy and security in the cloud are well recognized and have been extensively discussed in the business and popular press. However, one critical issue that has received very little attention with respect to cloud computing is export control.

In the broadest sense, export control relates to regulations that the United States and many other countries have put in place to restrict the export of various sensitive items, information, and software.

There is an inherent tension between cloud computing and export control. While the concept of the cloud is centered on the premise of removing the need to track the details of data movement among various destinations, export control regulations are built largely around restrictions tied to those very movements.

If cloud computing is to reach its full potential, it is critical for providers and users of cloud services to address its implications with respect to export control. It is equally important to adapt the export control regulations to reflect the increasing prevalence of cloud computing in a manner that preserves the ability of American companies to benefit from the efficiencies of the cloud while also ensuring that American national security and foreign policy interests are adequately protected.

John Villasenor is a nonresident senior fellow in Governance Studies and in the Center for Technology Innovation at Brookings. He is also professor of electrical engineering at the University of California, Los Angeles.

The Growth of Cloud Computing

Cloud computing involves on-demand access to a shared pool of configurable computing resources [Mel2009] for computation, storage, and other services and applications.

While the widespread use of the term "cloud computing" is new, techniques that are described today in terms of the cloud have existed for years and in some cases decades. A 1980s computer user who used a dial-up modem connection to read e-mail was accessing information that in today's parlance was "in the cloud." In fact, cloud-based methods go back to the earliest days of computers, as evidenced by a 1961 IBM announcement describing an airline reservation system that "assures that queries and entries from any point in the system, however remote, will receive a response from the data processing center within seconds" [Hea2002] – language that would not be particularly out of place half a century later in describing a current software-as-a-service cloud application.

What has changed is not the basic technological capability to deliver cloud-like computing functionality, but the speed, scale, diversity, and complexity of cloud computing offerings and the extent to which organizations of every type and size

are utilizing those offerings. In particular, the last several years has seen spectacular growth in the cloud both in terms of market size and adoption.

According to an April 2011 report from Forrester Research, the overall size of the cloud computing market will reach $40 billion in 2011 and grow to over $240 billion in 2020.[1] In a recent survey of over 400 users and vendors of cloud software, support and services and other industry experts [NBV2011], over 50 percent of the respondents stated that they performed more than half of their computing in the cloud today, and over 80 percent of the respondents expect to be performing more than half of their computing to the cloud within five years.[2] In addition, today's cloud-based networks are increasingly global.[3]

These changes are greatly increasing both the volume of transborder data flows and the number of people who have access to data moving through the cloud. This in turn, bears directly on the issue of export control, which as one of its central functions imposes restrictions on where certain data can move and who can access it.

Export Control

Export control in the United States plays a critical role in national security and foreign policy by placing restrictions on the broadly defined "export" of certain items, software, and technology.

Export control in the United States has a long history. In 1775, the year before the signing of the Declaration of Independence, Congress acted to bar the export of goods to Great Britain [NTIS2011]. Other notable export control legislation includes the Embargo Act of 1807 [Bri2011], the Trading with the Enemy Act of 1917, the Export Administration Act of 1969 [Mei2008], and the 2007 International Emergency Economic Powers Enhancement Act [BIS2011].

Today, export control oversight authority in the United States is held by the Departments of Commerce, Defense, State,[4] Treasury, Energy, and Interior; the Nuclear Regulatory Commission, the Environmental Protection Agency, the Food and Drug Administration, and other U.S. Government organizations [BIS2011a].

Given its importance, the issue of export control with respect to the cloud has not been given the attention it merits. It is widely recognized that the cloud raises complex policy questions of security [Bro2010, Car2011], privacy [Fri2010, Kat2010, Rui2011, Sva2010], and jurisdiction [Bra2011, Jae2009]. However, while these issues are related in various ways to export control, there are important differences as well. The concept of jurisdiction is often closely tied to location, and security and privacy are closely tied to access. By contrast, export control primarily addresses movement. If 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.

Companies that sell export-controlled products or services typically have well-

established internal procedures aimed at ensuring export control compliance. Such companies clearly need to be highly attentive to the ways they use cloud computing. What is less obvious is that companies that do not sell export-controlled products or services also need to consider export control regulations as they move to the cloud.

This is because the techniques used to process information in large, complex information technology environments may in some cases fall under the umbrella of export control regulations. In fact, ironically, in some instances the software methods explicitly implemented to take advantage of cloud-based computing environments could lead to export control violations when some components of the cloud are located abroad.

The civil and criminal penalties associated with export control violations can be significant. For example, in March 2010, British Company BAE Systems plc was ordered to pay a criminal fine of $400 million for actions that included export control violations [DOJ2010]. In October 2010, the owners of a California technology company were charged with conspiring to export restricted electronics technology to China – a count that carries a maximum penalty of 20 years in federal prison [USAO2011].

While cloud computing has implications for many forms of export control, the present paper considers the Export Administration Regulations[5] (EAR) overseen by the Bureau of Industry and Security within the U.S. Department of Commerce. The growth in cloud computing raises a number of important issues particularly relevant to the EAR for cloud service providers, users of those services, and regulators.

When Do Users of Cloud Services Become Exporters?

Users of cloud services far outnumber providers of those services, and interact with the cloud in an almost endless list of ways. Assessing export control from the standpoint of cloud users involves considering the types of actions users can take that can result in an export of data. To help illustrate the variety and complexity of the export control challenges with respect to cloud users, it is useful to consider several fact patterns:

> **Fact Pattern 1**: A user based in the U.S. contracts for cloud processing services with a U.S. provider that initially has servers located only in the U.S. The user sometimes processes EAR-restricted data in the cloud. Several months later, the provider opens a facility in Europe and starts taking on European customers. Unbeknownst to the user, the service provider then adopts a practice of taking advantage of the time zone differences between the United States and Europe to make more efficient use of its servers and reduce its infrastructure costs. During periods of high demand during the business day in the United States, some of the workload originating in the United States is moved to servers in Europe

where it is evening or night and demand is lower. Conversely during the business day in Europe, some of the workload originating in Europe is shifted to the United States where it is early morning.

In this fact pattern, export violations may be occurring on a daily basis, though neither the provider nor the user of the services are likely to be aware of this fact. In addition, since the physical location of the servers in the cloud is intentionally abstracted, the user of the cloud services may not be able to easily get information regarding where the computations are occurring.

> **Fact Pattern 2**: Person A, a U.S. citizen located in the United States, sends an e-mail containing EAR-restricted information in the body of the message to Person B, a U.S. citizen who normally works at a location in the United States. Unbeknownst to Person A, Person B is on a short trip overseas. Person B logs onto his e-mail while overseas using a public computer in the lobby of his hotel, sees that he has an e-mail message from Person A, but since he does not have any reason to believe in advance that it will contain EAR-restricted information, proceeds to click on the message and read it.

To the extent that this fact pattern is considered to be an export violation, who is the responsible party? Person A sent the information that was received abroad, but she did so on the good faith belief that it would be delivered to a U.S. citizen recipient within the United States. Person B downloaded the information from an e-mail server onto the computer in the lobby of the foreign hotel, but did so without any advanced indication or notice that the downloaded message might contain restricted information.

As a variant of this fact pattern, it also interesting to consider the case in which the e-mail service provider, noticing that Person B is logging into his e-mail from overseas, preemptively moves Person B's e-mails from a server in the United States to a server in the country where Person B is located to enable faster downloads to Person B. Even if Person B elects not to read the message from Person A, the EAR-restricted information has still been moved overseas.

Responsibilities in this variant of the fact pattern are even harder to identify. Person B did nothing more than log in to his e-mail and elect not to read a message from Person A. The e-mail service provider simply engaged in load balancing to improve its service quality, and was not aware that the information contained in the message from Person A had export restrictions.

> **Fact Pattern 3**: A company utilizing cloud-based infrastructure services runs a distributed computing application that includes EAR-restricted software. This software comprises a set of three different modules that run sequentially, and can be run on different servers. In the course of executing this software in the cloud, these modules are run on servers allocated by the cloud services provider. In some instances, the services provider allocates servers that are located outside the United States.

Under this fact pattern, when all three software modules are run on the same foreign server, an export control violation may well have occurred. However, things are more complex under other configurations. Suppose that the first software module is run overseas and the second and third modules are run in the United States. Suppose, further, that the first software module does nothing more than partition non-export-controlled data into a series of identically sized blocks as a first step in an otherwise export controlled encryption algorithm. In this case an argument might be made that no export control violation has occurred - after all, the partitioning of data into blocks occurs in hundreds of applications, the overwhelming majority of which are not subject to the EAR.

These two possibilities– one in which the full set of EAR-restricted software is shipped to the same foreign server for execution, and the other in which only an initial step involving a very common form of generic processing is run overseas – represent two points along a spectrum with many variations in between. Identifying where the export control lines lie in such scenarios is one of the most significant challenges facing users of cloud services and export control regulators.

Export Control and Cloud Service Providers

To date, the Department of Commerce Bureau of Industry and Security (BIS) has issued two Advisory Opinions related to cloud computing, both of which generally address export control issues from the standpoint of cloud service providers.

The first BIS Advisory Opinion [BIS2009] (hereafter the "2009 AO"), was published in January 2009, and considers whether the provision, as opposed to use, of cloud computing services would be subject to export control. In addressing this question, the 2009 AO distinguishes between providers that only sell computational capacity from those that both sell capacity and give users assistance in using it.

Specifically, the 2009 AO states, among other things, that "[t]he service of providing computational capacity would not be subject to the EAR as the service provider is not shipping or transmitting any commodity, software or technology to the user." However, the 2009 AO also states that if a service provider furnishes software, technical data, or technical assistance "that is not publicly available in order to give the user[s] knowledge on how to access and use the computational capacity provided by grid or cloud computing, then that technology would be subject to the EAR."[6]

The second Advisory Opinion [BIS2011b] (the "2011 AO") issued in January 2011 and considers, among other issues, "deemed exports." Under the EAR, the term export encompasses not only physical export from the United States, but also the "release of technology to a foreign national in the United States" (i.e., a deemed export).[7] This could occur if a foreign national working at the offices of an American cloud computing services provider in the United States were to receive export-controlled information through interactions with a user of the cloud

services.

Accordingly, the 2011 AO addresses whether cloud computing service providers need to "obtain deemed export licenses for foreign national information technology ('IT') administrators who service and maintain their cloud computing systems." In addressing this question, BIS once again made the distinction between the providers and users of cloud services, stating that "the service of providing computational capacity through grid or cloud computing is not subject to the EAR, since the service provider is not shipping or transmitting any commodity, software, or technology subject to the EAR to the user." The 2011 AO then notes that "[b]ecause the service provider is not an 'exporter,' " the company providing the cloud services "would not be making a 'deemed export' if a foreign national network administrator monitored or screened, as described above, user-generated technology subject to the EAR."

The export control elephant in the room in the fact pattern considered above concerns assigning responsibility for the deemed export that may occur when the foreign national network administrator monitors user-generated technology subject to the EAR. The only parties in the transaction are the service provider, the user, and the foreign national. While the 2011 AO is clear in stating that the service provider would not be making a deemed export under the fact pattern considered, a deemed export is exactly what may have occurred since the foreign national IT professional is now newly in possession of export controlled technology delivered to him or her in the United States through the collective infrastructure and actions of a cloud service provider and user. Putting aside the foreign national, who presumably cannot be found to have exported information to him or herself, this leaves the user as the only possible exporter.

In theory, a user based in the United States and contracting cloud services with a service provider also based in the United States could have inquired regarding the nationality of all the IT professionals employed or contracted by the service provider in advance. However, today's Service Level Agreements (SLAs) are generally silent on such points.

Moving Forward: Recommendations

As is clear from the foregoing discussion, cloud computing creates a greatly expanded set of mechanisms for the movement of export-controlled information abroad or the provision of that information to foreign nationals in the form of deemed exports. This creates an increased likelihood of unintentional export control violations as well as increased vulnerabilities with respect to the intentional export of controlled information.

Providers of cloud services, users of those services, and export control regulators can all play an extremely important role in effectively addressing export control given the move to the cloud.

Recommendations for Service Providers

Providers of cloud services should offer users the ability to exert some level of control over the physical location of cloud resources. In some cases, this may require interaction among multiple entities when a service provider does not directly control the infrastructure used in providing the services. While there are some models of cloud computing in which users can identify particular physical server and storage locations, many cloud services are performed under SLAs that provide details regarding the nature and reliability of the service but are silent on where the associated computing facilities are located.

Service pricing could in part reflect the extent of location control that the user is allowed to impose, involving a slight premium to ensure the assignment of servers based in the United States. In a large country such as the United States it will often be feasible for providers to offer this flexibility without significantly impacting the overall utilization efficiency of their computing resources; in small countries this is less practical.

A service provider that offers users the option to restrict their computations to servers in the United States can also expect that some users electing that option may also want assurances that they will not encounter deemed export problems in their routine customer support interactions with the service provider. Service providers that organize their staffing and internal access procedures accordingly will be more likely to win business from users with these concerns.

In addition, in light of the guidance in the 2009 AO from the Bureau of Industry and Security that the provision of "knowledge on how to access and use the computational capacity" provided by cloud computing is subject to the EAR, service providers transmitting such knowledge to their customers should review that information in advance to ensure that doing so will not result in any EAR violations.

This can be accomplished in several ways. First, traditional academic publications describing the results of basic research in venues such as conferences typically do not typically contain export-controlled information. There is a large and growing body of open literature regarding the efficient use of cloud computing environments, some of which may be relevant to support that cloud service providers can offer to their customers. Secondly, cloud service providers with an interest in providing assistance to users that may fall within the scope of the EAR may still be able to do so as long as they obtain appropriate licenses and exercise appropriate diligence with respect to recipients of that assistance.

Recommendations for Users of Cloud Services

For companies that sell export-controlled products or services, use of the cloud raises clear concerns. In some cases, however, such companies can still take advantage of some of the benefits of cloud computing by using appropriately structured private clouds.

For companies with a complex range of product and service offerings that in some but not all cases are restricted by the EAR, care needs to be taken that enterprise-wide moves to cloud computing environments do not create an increased risk of violations. One trend to be mindful of in this regard concerns the shift from private cloud solutions to hybrid or public cloud solutions. Corporate information technology professionals should ensure that all relevant stakeholders participate in any decisions to transition away from private cloud environments, and that the transition itself is performed with due attention to export control concerns.

As noted previously, even companies that do not sell export-controlled products or services need to be cognizant of export control as they move to the cloud. For example, the EAR include restrictions on software enabling the use of dynamic adaptive routing in a network[8] as well as on certain encryption methods.[9] Any company planning to deploy software employing restricted forms of encryption, dynamic adaptive routing, or other processing subject to the EAR on resources in the cloud should consider the associated export control implications.

To the extent that service providers offer users the option to pay a premium to ensure that data stored or transmitted on the provider's equipment will not be exported in any sense of the word, this offers a possible mechanism for the cloud-based processing of EAR-restricted data and the use of EAR-restricted methods. However, users should also be prepared for the small possibility that a provider may violate a contractual obligation to avoid export, either inadvertently, or intentionally to save costs. While various legal remedies to address this could be built into a contract, those remedies would not fully address liabilities and exposures from the standpoint of government enforcement of any resulting export control violations. In addition, a company identified as the source of export control violations could experience significant damage to its reputation and business prospects.

It is also important to update employee training and education programs to specifically address the implications of the cloud with respect to export control. Given the extremely fast pace of changes in the cloud computing ecosystem, briefings regarding export control compliance that were last updated as recently as two or three years ago are likely to give insufficient attention to current cloud computing issues.

Universities can be both providers and users of cloud services. Universities should avoid being lulled into complacency by the fundamental research exemption (FRE), which provides conditions, subject to certain important exceptions, under which the EAR do not apply to university research "where the resulting information is ordinarily published and shared broadly within the scientific community."[10]

University decisions regarding engagement with cloud computing driven by the fact that the majority of their science and engineering research falls under the FRE risk creating a higher likelihood of export control violations for the subset of their research that does not qualify for this exemption. A move to cloud-based

services in relation to non-export-controlled research increases the chances that those services will unintentionally be used for export-controlled research as well.

A further concern is that universities often have much more open and heterogeneous information technology systems than corporations. The mixing of such systems with cloud-based computing environments creates obvious concerns with respect to export-controlled information, and also leads to greater vulnerabilities with respect to the enormous volume of non-export-controlled - but still extremely valuable -intellectual property that is often stored on university information technology systems.

Recommendations for Regulators

A hands-off regulatory approach with respect to cloud computing would constitute a de facto weakening of U.S. export control regulations, as cloud computing has created numerous new vectors for information movement. However, if American companies are subject to overly conservative restrictions regarding cloud computing that greatly reduce their ability to benefit from its efficiencies, they will be less able to compete globally. While regulation is always an exercise in navigating tradeoffs, the tradeoffs at the intersection of cloud computing and export control are particularly nuanced.

Users of cloud services would benefit from regulatory guidance regarding whether it is ever permissible, and if so under what conditions, to execute portions of EAR-restricted software that involve generic computations commonly found in non-EAR-restricted applications on servers abroad.

Users would also benefit from regulatory guidance regarding whether the inability in some cloud service offerings to identify which individual computer server is being used for a particular computing function impacts the application of the EAR. There is some language in the 2009 AO suggesting that in at least some circumstances, the inability "to distinguish individual system access" may have some relevance with respect to the EAR. However, this language was provided in response to a specific, narrowly tailored question, and the 2009 AO does not address whether it might apply more broadly.[11]

An additional possible regulatory step involves updating export control regulations to support increased security of cloud-based applications. Many U.S. companies use today, or will soon use in the future, global cloud-based networks for storing non-export-controlled data. To the extent that current export control laws place an upper limit on the strength of the encryption that can be used to protect that data, the data is more vulnerable to intellectual property theft. In view of cloud computing and continued advances in encryption technology, it is worth at least considering whether the optimal regulatory "turn of the dial" regarding encryption strength restrictions should be moved.

Alternatively or in addition, it may also be worth examining whether the current EAR encryption restriction carve-outs available in relation to certain types of smart cards and banking transactions should be broadened to also encompass

some non-banking cloud-based data transactions.

Another area in which regulatory guidance would be beneficial concerns the application of *de minimis* rules in cloud computing systems, both from the standpoint of providers and users.

Multilateral export control aspects of cloud computing can also be addressed. For example, the Wassenaar Arrangement[12] includes several technology categories that are highly relevant to cloud computing. To the extent that U.S. export control regulations are updated in view of cloud computing, it would be appropriate to propose corresponding updates through regimes such as the Wassenaar Arrangement as well.

Conclusions

Cloud computing is reshaping the landscape with respect to business, government, university, and consumer information technologies, delivering increased flexibility and improved cost efficiencies for a wide range of services. Along with its many advantages, however, the move to the cloud also creates new mechanisms for the unintentional or intentional export of software and technology subject to export control regulations.

Given the importance of export control in protecting American national security and foreign policy interests, it is incumbent on all participants in the cloud computing ecosystem to examine their use of the cloud to ensure compliance with existing export control regulations, and to minimize the opportunities for cloud-based systems to be exploited in violation of those regulations. Regulators can also play an important role in providing guidance and potentially in updating regulations to help American businesses benefit from cloud computing while also maintaining appropriate protections against the unauthorized export of sensitive software and technology.

Governance Studies
The Brookings Institution
1775 Massachusetts Ave., NW
Washington, DC 20036
Tel: 202.797.6090
Fax: 202.797.6144
www.brookings.edu/governance.aspx

Editor
Christine Jacobs

Production & Layout
John S Seo

E-mail your comments to gscomments@brookings.edu

Endnotes

[1] "Forrester forecasts USD 241 billion cloud computing market by 2020." Information Week News Network, April 26, 2011. http://www.informationweek.in/Cloud_Computing/11-04-26/Forrester_forecasts_USD_241_billion_cloud_computing_market_by_2020.aspx, retrieved July 7, 2011.

[2] "Future of Cloud Computing." http://futureofcloudcomputing.drupalgardens.com/2011-future-cloud-computing-survey-results, retrieved July 7, 2011, slide 34. Overall survey results are at http://futureofcloudcomputing.drupalgardens.com/2011-survey.

[3] See, for example, the AT&T press release *AT&T Targets Close to $1 Billion of Investment to Deploy Global Network-Based Cloud and Mobility Solutions for Businesses.* Dallas, May 10, 2011. http://www.corp.att.com/emea/insights/pr/eng/1billion_cloud_100511.html, retrieved July 10, 2011.

[4] The Department of State administers the International Traffic in Arms regulations (ITAR). See 22 C.F.R. § 120 – 130 and http://www.pmddtc.state.gov/regulations_laws/itar_official.html .

[5] The Export Administration Regulations (EAR) are provided in the Code of Federal Regulations (CFR), Title 15 ("Commerce and Foreign Trade"), Volume 2, Chapter VII, Subchapter C, Parts 730-774 (denoted 15 C.F.R. § 730-774). An unofficial version of the CFR is provided through the Electronic Code of Federal Regulations (e-CFR) by the Government at http://ecfr.gpoaccess.gov. Supplement Number 1 to § 774 of the EAR is the Commerce Control List (CCL), which describes restricted commodities, software, and technology. The terms "technology", "software", and "commodities" have special meanings in the context of the EAR. See 15 C.F.R. § 772.1: "Definitions of terms as used in the Export Administration Regulations (EAR)." "Technology" is defined to include "[s]pecific information necessary for the 'development', 'production', or 'use' of a product," in the form of technical data or technical assistance such as instruction, skills training, or consulting services. Software is "[a] collection of one or more 'programs' or 'microprograms' fixed in any tangible medium of expression." Commodities are defined as "[a]ny article, material, or supply except technology and software."

[6] An additional area of service provider responsibility identified in the 2009 Advisory Opinion relates to 15 C.F.R. § 744.6(a)(2), which places restrictions regarding knowingly providing assistance in the "design, development, production, or use of missiles" in or by a restricted country, or in the "design, development, production, stockpiling, or use of chemical or biological weapon in or by any country or destination, worldwide." As BIS explained in the 2009

Advisory Opinion, §744.6(a)(2) "can have broad application because it applies to activities unrelated to exports, such as services" and in addition "can apply to items that are not subject to the EAR." In addition, the 2009 Advisory Opinion then explains that "service providers must have knowledge, as that term is defined in § 772.1, that the service will directly assist in those activities described in § 744.6(a)(2) before that restriction will apply."

[7] The term "export" has a broad meaning under the EAR, encompassing not only physical export from the United States, but also the re-export to a third country of "commodities, software, and technology that have been exported from the United States" to a second country, the "release of technology to a foreign national in the United States" (i.e. a deemed export), and "the electronic transmission of non-public data that will be received abroad." See 15 C.F.R. §730.5 "Coverage of more than exports."

[8] See Supplement Number 1 to Part 774 of the EAR (The Commerce Control List), Category 5 - Telecommunications and "Information Security", Section I. Telecommunications, Sections 5A991 (e) (2) and 5D991.

[9] See Supplement Number 1 to Part 774 of the EAR (The Commerce Control List), Category 5 - Telecommunications and "Information Security", Section II. "Information Security."

[10] Fundamental Research under the EAR is addressed in 15 C.F.R. § 734.8. Fundamental research under the Department of State International Traffic in Arms Regulations (ITAR) is addressed in 22 C.F.R. § 120.11.

[11] The cited portion of the 2009 Advisory Opinion discusses the relevance of the ability "to distinguish individual system access" in relation to 15 C.F.R. § 740.7(b)(2), which prohibits the release of certain technology and source code to nationals of Cuba, Iran, North Korea, Sudan, or Syria.

[12] The Wassenaar Arrangement currently has about 40 member states including the United States, and promotes "transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies." See http://www.wassenaar.org/introduction/index.html, retrieved July 4, 2011. Categories of goods and technologies in the December 2010 Wassenaar Arrangement Control List particularly relevant to cloud computing include Category 4 ("Computers") and Category 5 Part 1 ("Telecommunications"), and Category 5 Part 2 ("Information Security"). See http://www.wassenaar.org/controllists/index.html.

Cited References

[BIS2009] Bureau of Industry and Security, January 13, 2009 Advisory Opinion on the application of EAR to grid and cloud computing services. http://www.bis.doc.gov/policiesandregulations/advisoryopinions/jan13_2009_ao_on_cloud_grid_computing.pdf, retrieved July 7, 2011.

[BIS2011] Bureau of Industry and Security. *Other Related Enforcement Topics.* http://www.bis.doc.gov/complianceandenforcement/othereetopics.htm, retrieved July 11, 2011.

[BIS2011a] Bureau of Industry and Security. *United States Government Departments and Agencies with Export Control Responsibilities.* http://www.bis.doc.gov/about/reslinks.htm, retrieved July 6, 2011.

[BIS2011b] Bureau of Industry and Security, January 11, 2011 Advisory Opinion on the issue of cloud computing and deemed exports. http://www.bis.doc.gov/policiesandregulations/advisoryopinions/jan11_2011.pdf, retrieved July 7, 2011.

[Bra2011] Bradshaw, Simon, Christopher Millard, and Ian Walden. "The Terms They Are A-Changin'... Watching Cloud Contracts Take Shape." *Brookings Institution Issues in Technology Innovation* 7 (2011). http://www.brookings.edu/papers/2011/03_cloud_computing_contracts.aspx, retrieved July 7, 2011.

[Bri2011] "Embargo Act." *Encyclopædia Britannica. Encyclopædia Britannica Online,* 2011. http://www.britannica.com/EBchecked/topic/185515/Embargo-Act, retrieved July 9, 2011.

[Bro2010] Brock, Michael and Andrzej Goscinski. "Toward a Framework for Cloud Security." Algorithms and Architectures for Parallel Processing, ICA3PP 2010. Ed. Ching-Hsien Hsu et al. Berlin:Springer, 2010, 254-263. http://www.springerlink.com/content/x7042k211587285u/, retrieved July 11, 2011.

[Car2011] Carlin, Sean and Kevin Curran. "Cloud Computing Security." *International Journal of Ambient Computing and Intelligence* 3:1 (2011): 38-46. http://www.infm.ulst.ac.uk/~Kevin/ijacivol3no1.pdf, retrieved July 11, 2011.

[DOJ2010] Department of Justice. *BAE Systems PLC Pleads Guilty and Ordered to Pay $400 Million Criminal Fine.* Washington, DC, March 1, 2010.

http://www.justice.gov/opa/pr/2010/March/10-crm-209.html, retrieved July 9, 2011.

[Fri2010] Friedman, Allan A. and Darrell M. West. "Privacy and Security in Cloud Computing." *Brookings Institution Issues in Technology Innovation* 3 (2010). http://www.brookings.edu/papers/2010/1026_cloud_computing_friedman_west.aspx, retrieved July 7, 2011

[Hea2002] Head, Robert. "Getting Sabre off the Ground." *IEEE Annals of the History of Computing* 24:2 (2002): 32-39.

[Jae2009] Jaeger, Paul T., Jimmy Lin, Justin M. Grimes, and Shannon N. Simmons. "Where is the cloud? Geography, economics, environment, and jurisdiction in cloud computing." *First Monday* 14:5 May 2009. http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2456, retrieved July 7, 2011.

[Kat2010] Katzan, Harry Jr. "On The Privacy Of Cloud Computing." *International Journal of Management and Information Systems* 14:2 (2010): 1-12. http://journals.cluteonline.com/index.php/IJMIS/article/view/824/808, retrieved July 7, 2011.

{Mei2008] Meixner, Charles. "Export Control; What's It All About?" *Defense Technical Information Center 2008 Conference: Protecting While Sharing Defense Information, April 7-9, 2008*. www.dtic.mil/dtic/ppt/2008ppt/ExportControl.ppt, retrieved July 9, 2011.

[Mel2009] Mell, Peter and Tim Grance. "The NIST Definition of Cloud Computing, Version 15." The National Institute of Standards and Technology. October 7, 2009. http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf, retrieved July 7, 2011.

[NBV2011] North Bridge Venture Partners. *Future of Cloud Computing Survey Reveals New Drivers for Cloud Adoption.* San Francisco, June 22, 2011. http://www.businesswire.com/news/home/20110622006602/en/Future-Cloud-Computing-Survey-Reveals-Drivers-Cloud, retrieved July 7, 2011

[NTIS2011] National Technical Information Service. *History of Export Controls*. https://bxa.ntis.gov/mission.html, retrieved July 9, 2011.

[Rui2011] Ruiter, Joep and Martijn Warnier, "Privacy Regulations for Cloud Computing: Compliance and Implementation in Theory and Practice." *Computers, Privacy, and Data Protection: An Element of Choice*. Ed. S. Gutworth, Y Poullet, P. De

Hert, and R. Leenes. Dordrecht:Springer, 2011. 361-376. http://www.springerlink.com/content/t214883333672582/, retrieved July 7, 2011.

[Sva2010] Svantesson, Dan and Roger Clarke. "Privacy and consumer risks in cloud computing." *Computer Law Security Review* 26:4 (2010): 391-97. http://www.sciencedirect.com/science/article/pii/S0267364910000828, retrieved July 7, 2011.

[USAO2010] United States Attorney's Office, Central District of California, *California Couple Charged With Conspiring to Export Sensitive Technology to People's Republic of China.* Los Angeles, October 15, 2010. http://www.justice.gov/usao/cac/pressroom/pr2010/149.html, retrieved July 9, 2011.