SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 28 SPRING 2013 ARTICLE 3, PAGE 65

U.S. Export Controls Over Cloud Computing: The Forecast Calls for Change

Ryan M. Murphy*

TABLE OF CONTENTS

INTRODUCTION

Are you violating United States export law when you click "save" on that document? Exactly where does that file go? For some, it may travel to a server within their company's building, but for an increasing population, that file goes "into the clouds" and out of the country. If you use a service provider to host e-mail or store data, it's important to understand the type of data you are storing and where that information is located. Many cloud providers utilize a vast array of servers, referred to commonly as "clouds", located all over the world.[1] These servers are connected and work together to provide a seamless hosting environment for users.[2] A significant export control issue arises when the data stored on a cloud falls within the type regulated by the Export Administration Regulations ("EAR"), and it's sent to a server in another country.[3] If so, you may have just unknowingly exported your data and become subject to government regulation.

With the global market for cloud computing services projected to grow from $68 billion in 2010 to almost $150 billion in 2014 and the Obama administration's plans to move a significant portion of its IT capabilities to a cloud within 14 months,[4] there is a great need for reform in the United States' outdated export law. The United States enacted the current Export

---

* Syracuse University College of Law, Juris Doctorate Candidate 2013

[1] Tom Reynolds, *Cloudy Answers on Cloud Computing*, http://www.exportsolutionsinc.com/blog/cloudy-answers-on-cloud-computing/ (last visited Feb 6., 2012).

[2] One day your data may be located in Massachusetts, the next day it may be sent to a server in Amsterdam, and the next day sent to a server in India and so on.

[3] This applies even if an e-mail is sent from a United States location through a foreign server to another United States location.

[4] Nixon Peabody, *The Export Control Implications of Cloud Computing*, 41 No. 17 THE LAWYER'S BRIEF 2.

Administration Act ("EAA of 1979") in 1979, and has made no significant change since. In fact, EAA of 1979 has been expired for a significant time, but regulations created under it remain in force pursuant to a separate emergency power statute.[5] Since 1979, our society has become fully integrated with technology and the vast majority of businesses now use computers, e-mail, and the Internet daily. We are no longer the society cut off from the world we once were in 1979, but our current law does not reflect this evolution.[6] From this, a tension exists between cloud computing and export control that must be handled in a way that allows cloud computing to reach its potential, but still gives reasonable protections to the United States.

Part I of this Note frames the issue by providing relevant background information on the development and current landscape of U.S. export control laws. Part II then provides a detailed overview of cloud computing and the different options a business has in its use of the technology. Part III examines the current application of U.S. export control law on cloud computing and discusses implications that may arise in different scenarios. In Part IV, this Note looks to the United Kingdom and the European Union and gleans potential initiatives the U.S. government should implement to revise the outdated U.S. export control law. Part V posits three specific fixes the government must implement to correct the U.S. export control system. Lastly,

---

[5] 50 U.S.C. § 2419 (2013); Gregory W. Bowman, *E-Mails, Servers, and Software: U.S. Export Controls for the Modern Era*, 35 GEO. J. INT'L L. 319, 324 (2004); International Emergency Economic Powers Act, 50 U.S.C. §§ 1701-1707 (2013).

[6] See Advisory Opinion from C. Randall Pratt, Director, Information Technology Controls Center, Office of National Security and Technology Transfers Control, Bureau of Industry and Security (Jan. 11, 2011) (available at http://www.bis.doc.gov/policiesandregulations/advisoryopinions/jan11_2011.pdf) and Advisory Opinion from C. Randall Pratt, Director, Information Technology Controls Center, Office of National Security and Technology Transfers Control, Bureau of Industry and Security (Jan. 13, 2009) (available at http://www.bis.doc.gov/policiesandregulations/advisoryopinions/jan13_2009_ao_on_cloud_grid_computing.pdf) (two advisory opinions have been given on the effect cloud computing has had on the meaning of the term "export," but no unified position has been given by the government).

this Note concludes by recommending the complete revamping of U.S. export control law in order to create a more efficient system that will allow cloud computing to reach its full potential.

I. U.S. EXPORT CONTROL LAWS AND REGULATIONS

The U.S. Constitution vests Congress with the power to "regulate commerce with foreign nations."[7] Specifically, this clause of the Constitution gives Congress power to regulate the exportation of domestic goods abroad. With this ability, Congress passed the EAA of 1979 and the International Emergency Economic Powers Act ("IEEPA").[8] These acts authorized multiple federal agencies, namely the Department of Commerce, to oversee and to regulate the exportation of commodities, software, and technology.[9] It is important to note, however, that the act terminated on September 30, 1990, but President Bush issued an executive order to extend it in its original form until Congress produced new legislation (which has still yet to occur).[10] Congress had three major goals when they passed EAA of 1979: enhance national security,[11] allow for the use of exports as a foreign policy tool, and restrict exports in short supply.[12]

---

[7] U.S. CONST. art. II, § 8.

[8] EAA of 1979, 50 U.S.C. § app. 2403; the International Emergency Economic Powers Act, 50 U.S.C. §§ 1701-1707.

[9] *Id;* Karen R. Smith, *A Basic Discussion of U.S. Export Regulations: What Every Client Needs to Know*, 1 J. TRANSNAT'L L. & POL'Y 113 (1992) ("The federal government regulates all exports, and authority for overseeing and regulating exports is divided among a number of agencies . . . the Department of Commerce, [] is a 'catch all' agency charged with regulating virtually all exports not regulated by any other agency . . . .").

[10] *See* 15 C.F.R. § 770.3(a) (1991)*;* Exec. Order No. 12,730, 3 C.F.R. §305 (1991).

[11] Karen R. Smith, *A Basic Discussion of U.S. Export Regulations: What Every Client Needs to Know*, 1 J. TRANSNAT'L L. & POL'Y 113 (1992) (National Security encompasses products that contribute to the military potential of any other country which hurt U.S. national security, such as software, computers, and electrical equipment. This is closely tied to foreign policy restrictions.).

[12] 50 U.S.C. app. § 2402(2); Gregory W. Bowman, *E-Mails, Servers, and Software: U.S. Export Controls for the Modern Era*, 35 GEO. J. INT'L L. 319, 329 (2004).

Though multiple agencies regulate the exportation of domestic products since the passing of the EAA of 1979, the Department of Commerce has lead the government's enforcement and regulation of non-physical exports today. Specifically, the Department of Commerce's Bureau of Industry and Security ("BIS") administers the specific regulations implemented by the EAA of 1979.[13] These regulations are administered through the use of EAR.[14] The US government, however, does not actively enforce the regulations defined in the EAR.[15] The EAR only recommends parties involved in export transactions analyze the nature of the product they are exporting and then determine, on their own, whether a license[16] would in fact be required.[17]

The EAR defines an export as "an actual shipment or transmission of items [including technology or software subject to the EAR] out of the United States."[18] Additionally, the EAR provides that "an actual shipment *or transmission* of items subject to the EAR out of the United States, or *release of technology or software* subject to the EAR to a foreign national in the United States . . ." (emphasis added).[19] Further, BIS maintains a list of the technologies subject to the

---

[13] Bureau of Industry and Security Export Administration Regulations, 15 C.F.R. §§ 730-774.

[14] *Id.*

[15] *See* 15 C.F.R. §§ 732.1(b)-(c); Gregory W. Bowman, *E-Mails, Servers, and Software: U.S. Export Controls for the Modern Era*, 35 GEO. J. INT'L L. 319, 332-33 (2004).

[16] 15 C.F.R. § 770.3(a) (1991) ("[T]he export from the United States of all commodities, and all technical data . . . is hereby prohibited unless and until a general license authorizing such export shall have been established or a validated license or other authorization for such expert shall have been granted . . . .").

[17] Gregory W. Bowman, *E-Mails, Servers, and Software: U.S. Export Controls for the Modern Era*, 35 GEO. J. INT'L L. 319, 332-33 (2004).

[18] 15 C.F.R. § 772.1 (2013) (The term "subject to the EAR" is a defined term of art in the EAR used "to describe those commodities, software, technology, and activities over which [BIS] exercises regulatory jurisdiction under the EAR.")

[19] 15 C.F.R. §734.2(b)(1) (2013).

EAR.[20] This list is known as the Commerce Control List ("CCL"), and is contained within the EAR.[21] The restrictions on items listed in the CCL depend on the location where the item is being exported or the nationality of the person to whom it is being sent.[22]

To clarify its regulations, the EAR puts forth five questions for exporters to consider when determining the need for a license: (1) is the item subject to the EAR; (2) how is the item classified for EAR purposes; (3) what is the item's ultimate destination; (4) what parties are involved in the transaction and are any of the parties restricted; and (5) what is the intended end use of the item?[23] The EAR applies to all civilian and "dual use"[24] commodities,[25] software,[26] and technology[27] not publically available.[28] In essence, the government shifts the burden to comply with the regulations set forth in EAR onto the exporter. Though self-regulating, the penalty for violating the EAR can range up to $50,000 and/or imprisonment for up to five years.[29]

---

[20] 15 C.F.R. §738.1 (2013).

[21] 15 C.F.R. §774 (2013).

[22] 15 C.F.R. §738.1 (2013).

[23] Gregory W. Bowman, *supra* note 17 at 333-34.

[24] *See* 15 C.F.R. § 772.1 (2013) (dual use refers to "[i]tems that have both commercial and military or proliferation applications.").

[25] *Id.* (EAR defines commodity as "[a]ny article, material, or supply except technology and software").

[26] *Id.* (EAR defines software as a "collection of one or more 'programs' or 'microprograms' fixed in any tangible means of expression.").

[27] *Id.* (EAR defines technology as "[s]pecific information necessary for the 'development', 'production', or 'use' of a product," and this information can "take[] the form of 'technical data' or 'technical assistance.'")

[28] Bowman, *supra* note 17 at 319, 334.

[29] *See* 15 C.F.R. § 764.3(b).

II. OVERVIEW OF CLOUD COMPUTING

Cloud computing[30] describes the use of technology that allows users to access services over the Internet without the need to control the infrastructure that provides the services.[31] In essence, it is computing on demand that makes applications and storage from remote computers accessible at anytime and from anywhere.[32] In public or community clouds (the focus of this note), a third-party vendor ("provider") owns or controls the remote hardware, software, and facilities[33], and the cloud computer user ("user") may access or upload that data anywhere and at any time. To be specific, providers offer services, such as server space or tools for software development, to the public and users can be individuals, companies of any size, or government agencies.[34] Common examples of public cloud services are e-mail message storage on remote servers by companies such as Google, Web 2.0, and services such as Facebook that provide storage of social networking information.[35]

---

[30] The term cloud computing "comes from the early days of the Internet where we drew the network as a cloud . . . we didn't care where the messages went . . . the cloud hid it from us." Kevin Marks, Google

[31] 14 No. 5 CYBERSPACE LAW 1; *See, e.g., In re* Google, Inc. & Cloud Computing Servs. (Mar. 17, 2009) ("Cloud Computing Services are an emerging network architecture by which data and applications reside on third party servers, managed by private firms, that provide remote access through web-based devices."), *available at* http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf; Robert Gellman, World Privacy Forum, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, WORLD PRIVACY FORUM, 4 (2009) ("[C]loud computing involves the sharing or storage by users of their own information on remote servers owned or operated by others and accessed through the Internet or other connections.").

[32] 14 No. 5 CYBERSPACE LAW 1.

[33] Shannon Brown, *Navigating the Fog of Cloud Computing Cloud Computing May Raise Ethical Questions. It Also Requires Technical Competence. Are You Ready?*, PA. LAW., September/October 2011, at 18, 19.

[34] *US Export Controls and Cloud Computing*, LAW360, published September 10, 2010, available at http://www.law360.com (last visited Feb. 6, 2012).

[35] *Id.*

Cloud computing has become a popular alternative for business because of a cloud's scalability, virtualized resources, and portability.[36] This is because the cloud's routers, servers, and technical data storage devices are generally located across multiple systems and taken care of by a third-party.[37] In fact, most companies generally do not know where their data will be stored within the cloud.[38] Cloud computing services are analyzed in the context of two important models of categorization: service models and deployment models.[39]

A. *Cloud Computing Service Models*

Clouds may be classified into different categories by the functions they perform for the user. Four standard types of "Service Models" currently exist[40]: Software-as-a-Service ("SaaS"), Storage-as-a-Service ("STaaS"), Platform-as-a-Service ("PaaS"), and Infrastructure-as-a-Service ("IaaS")[41]. SaaS and StaaS will be the focus of discussion in this note because of the public nature of the provider. While Paas and Iaas are important in the field of cloud computing, they do not deal with public use[42] and will therefore not be discussed in detail.[43]

---

[36] *The Export Control Implications of Cloud Computing*, *supra* note 4.41 No. 17 THE LAWYER'S BRIEF 2.

[37] *Id.*

[38] *Id.*

[39] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEPARTMENT OF COMMERCE, SPECIAL PUBLICATION 800-145, *The NIST Definition of Cloud Computing* (September 2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[40] Providers have the option to combine any attribute from the four types available to create a hybrid.

[41] Shannon Brown, *Navigating the Fog of Cloud Computing Cloud Computing May Raise Ethical Questions. It Also Requires Technical Competence. Are You Ready?*, PA. LAW., September/October 2011, at 18, 19 (2011).

[42] 14 No. 5 CYBERSPACE LAW 1 (IaaS allows people to rent services such as processing, storage and network capacity and PaaS allow developers to create applications that run in and use services provided from the cloud).

SaaS and STaaS provide users with two different, but important abilities. First, SaaS allows for organizations to pay for the use of servers to store their software application for third-party desktop users to access (for a price) without having to install the software.[44] In this model, the user does not control the underlying cloud infrastructure (i.e. the network, servers, operating systems, storage).[45] An example of this service model may be seen in Google Apps. In Google Apps, companies may upload their software onto Google's server for a cost and then Google allows for the public to access the software without forcing them to download it onto a computer.[46]

On the other hand, STaaS allows for online backups, data synchronization and file storage with sharing capabilities.[47] This type of cloud allows for users to backup data on a third-party server and creates the ability to access that information from mobile electronic devices.[48] An example of this service model may be seen in Apple Computer's MobileMe. MobileMe allows for individuals to backup their data stored on a personal computer and then access that data from anywhere at any time.[49]

---

[43] National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-145, *The NIST Definition of Cloud Computing* (September 2011) (PaaS: "The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services and tools supported by the provider") (IaaS: "The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software").

[44] 14 No. 5 CYBERSPACE LAW 1; Brown, *supra* note 41, at 18-19.

[45] National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-145, *The NIST Definition of Cloud Computing* (September 2011).

[46] *See* http://www.google.com/apps/intl/en/business/index.html (last visited Feb. 7, 2012).

[47] Brown, *supra* note 41 at 18, 19.

[48] *Id.*

[49] *See* http://www.apple.com/mobileme (last visited Feb. 7, 2012).

B. *Cloud Computing Deployment Models*

A cloud may also be categorized through the way in which it is shared (or not) between different users. There are four different "deployment models" a cloud may be defined as: a private cloud, a public cloud, a community cloud, and a hybrid cloud.[50]

In a private cloud, the infrastructure is owned by, or operated for, a single user. This cloud may, however, be owned, managed, and operated by the organization, a third party, or a combination of the two.[51] The location of the cloud may exist on or off the premises.[52]

In a public cloud, however, the infrastructure is open to the general public and shared between multiple unique users.[53] This open cloud means the users will be forced to operate the same hardware and software within the same database.[54] This model exists on the premises of the cloud provider.[55] A common example of such a cloud may be seen with e-mail servers such as Google or with data storage such as Apple's MobileMe.

In a community cloud, the third type of deployment, the infrastructure is owned by and operated for a limited set of users.[56] These users, such as a national government, generally hold

---

[50] W. Kuan Hon & Christopher Millard, *Data Export in Cloud Computing, How can Personal Data be Transferred outside the EEA?*, Queen Mary University of London School of Law Legal Studies Research Paper No 85/2011, available at: http://ssrn.com/abstract=1925066 (last visited Feb. 6, 2012).

[51] National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-145, *The NIST Definition of Cloud Computing* (Sept. 2011).

[52] *Id.*

[53] Kuan Hon, *supra* note 50. See also, National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-145, *The NIST Definition of Cloud Computing* (September 2011).

[54] *Id.*

[55] National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-145, *The NIST Definition of Cloud Computing* (September 2011).

[56] Kuan Hon, *supra* note 50.

a common interest (e.g., mission, security requirements, and compliance considerations).[57] For example all Government organizations within the state of Massachusetts may share computing infrastructure on the cloud to manage data related to citizens residing in Massachusetts.

In a hybrid cloud, the infrastructure is owned and operated for a specific user, but when necessary the user may process activities in a public cloud.[58] This cloud may be owned, managed, and operated by the organization, a third party, or a combination of the two.[59] The location of the cloud may exist on or off the premises.[60]

III. U.S. GOVERNMENT'S RESPONSE TO EXPORTATION VIOLATIONS IN THE CLOUDS

With the boom in technology from the enactment of the EAA of 1979, regulation of exports has attempted to expand with it. This has shown itself in the widening types of goods deemed to be exports as well as tweaks to the language within statutes to encompass non-tangible goods such as software.[61] Though multiple government agencies regulate domestic exports in the United States, only the BIS has attempted to answer the mounting questions swirling around cloud computing technology.[62] Specifically, the BIS issued two advisory

---

[57] Kuan Hon, *supra* note 50.

[58] *Id.*

[59] National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-145, *The NIST Definition of Cloud Computing* (September 2011).

[60] *Id*.

[61] *See* 15 C.F.R. § 770.

[62] Nixon Peabody, *The Export Control Implications of Cloud Computing*, 41 No. 17 THE LAWYER'S BRIEF 2.

opinions on cloud computing in 2009 and most recently in 2011.[63] With confusion created from the seemingly unknown new technology, these opinions were intended to guide the public in the application of EAR guidelines regarding technology products in the clouds.[64] However, it is important to note that these advisory opinions are not binding law, and only the BIS's perspective on the potential legal issues that may arise with cloud technology.

A. *2009 BIS Advisory Opinion*

BIS first submitted an advisory opinion ("2009 AO") on the application of the EAR to cloud computing technology in 2009.[65] In this opinion, BIS commented on some basic definitional issues and made it quite clear the user, and not the provider, of the cloud technology will be responsible for abiding by EAR.[66] In essence, 2009 AO made four important comments on cloud technology.[67] First, BIS stated that providing cloud technology is not an export nor is it subject to EAR.[68] Second, a user transmitting controlled software to a foreign destination[69] to enable cloud computing is subject to the EAR.[70] Third, exporting controlled software or

---

[63] BIS ADVISORY OPINION ON CLOUD COMPUTING, 984 PLI/Pat 985 (2009); BIS ADVISORY OPINION ON CLOUD COMPUTING, 992 PLI/Pat 982 (2011).

[64] Nixon Peabody, *The Export Control Implications of Cloud Computing*, 41 No. 17 THE LAWYER'S BRIEF 2.

[65] BIS ADVISORY OPINION ON CLOUD COMPUTING, 984 PLI/Pat 985 (2009).

[66] *Id.*

[67] Nixon Peabody, *The Export Control Implications of Cloud Computing*, 41 No. 17 THE LAWYER'S BRIEF 2.

[68] BIS ADVISORY OPINION ON CLOUD COMPUTING, 984 PLI/Pat 985 (2009).

[69] This also applies to transmitting software to a foreign national within the US and the routing of software through a foreign location.

[70] BIS ADVISORY OPINION ON CLOUD COMPUTING, 984 PLI/Pat 985 (2009).

technology to and from a cloud is subject to the EAR.[71] Fourth, the cloud provider in the US is not the exporter of any data that users place on and retrieves from their cloud.[72] Analyzing this advisory comment in light of the EAA of 1979 and the EAR, BIS makes its desire for self-regulated compliance quite clear. BIS's 2009 AO again puts the onus on the user to stay within the export laws and seemingly leaves them out in the rain.

B. *2011 BIS Advisory Opinion*

In January 2011, BIS submitted a second advisory opinion, but this comment focused on whether cloud providers need to obtain "deemed export" licenses[73] for their foreign national IT administrators who have access to the users' controlled technology ("2011 AO").[74] Generally under EAR, a foreign national, even when within the boarders of the United States, must have a license approved by the BIS in order to access certain products deemed restricted. However, in the 2011 AO, BIS determined this regulation did not pertain to the provider of the cloud.[75] With seemingly no regulations on the provider, the 2011 AO stretches the responsibilities of the user even more. In essence, because the provider has no culpability in regards to the product being

---

[71] BIS ADVISORY OPINION ON CLOUD COMPUTING, 984 PLI/Pat 985 (2009).

[72] *Id.*

[73] *See* 15 C.F.R. §734.2(b); Bowman, *supra* note 17 at 319, 338-40 ("[I]n addition to applying to physical and non-physical exports and re-exports, the EAR also expressly state that a 'release' of 'source code' software or technology to a foreign national who is not a permanent resident of the United States or a protected individual under U.S. immigration laws is deemed to be an export to the foreign national's home country [last country of citizenship or permanent residence], even when the release occurs entirely within national borders.").

[74] BIS ADVISORY OPINION ON CLOUD COMPUTING, 992 PLI/Pat 982 (2011); Nixon Peabody, *The Export Control Implications of Cloud Computing*, 41 No. 17 THE LAWYER'S BRIEF 2.

[75] BIS ADVISORY OPINION ON CLOUD COMPUTING, 992 PLI/Pat 982 (2011).

stored on their server or routed through their system, it becomes the responsibility of the user to ensure that its data is not accessible by any foreigners.[76]

C. *Cloud Computing Implications Under EAR's Advisory Opinions*

Both advisements have provided insight into the BIS's perspective on legal issues created by cloud computing technology, but they only addressed a limited range of scenarios. The main lesson to glean from these advisements is this: the sole burden of compliance with the EAR falls onto the *user* of cloud computing services and *not* the provider.[77] Each of the Advisory Opinions has its own subtle comment on this major fact and each address it at a different angle.

In the 2009 AO, the BIS provides that the provider is *not* an exporter because providing computational capacity, by itself a service, does not qualify as an exportation because it does not receive "the primary benefit of the transaction."[78] For example, if a U.S. based company decides to use a cloud provider that happens to have their servers based in the Netherlands, they will be responsible for this "export" even though they did not intend to export any product but only put the product on the third-party server to store it. However, according to the BIS, the company in this situation receives the primary benefit of this export and therefore has the obligation to abide by the U.S. export control laws and is responsible from protecting the data or product from foreign entities. In fact, the provider does not even have an obligation to inform the user of the location of their servers and if they reside outside of the United States.[79]

---

[76] This includes even the provider's own employees; Nixon Peabody, *The Export Control Implications of Cloud Computing*, 41 No. 17 THE LAWYER'S BRIEF 2.

[77] *See* BIS ADVISORY OPINION ON CLOUD COMPUTING, 984 PLI/Pat 985 (2009); BIS ADVISORY OPINION ON CLOUD COMPUTING, 992 PLI/Pat 982 (2011).

[78] BIS ADVISORY OPINION ON CLOUD COMPUTING, 984 PLI/Pat 985 (2009).

[79] *Id.*

The BIS addressed a similar issue in their 2011 AO. In it, the BIS broke down the obligations of users and providers when dealing with the provider's own foreign employees and tackled the question of who had the onus to protect technology from "deemed exports."[80] The issue arose from cloud providers and their foreign IT administrators' potential use of the user's data or product (which would be a deemed an export within or outside of the United States).[81] In this scenario, the 2011 AO, again, essentially put the entire burden on the user to protect their data or product from the provider's potentially foreign employees.[82]

These base rules taken from the Advisory Opinions create issues for the user in four different situations: (1) the provider's servers or resources are abroad and the user is in the United States; (2) the provider's servers or resource are in the United States and the user is abroad; (3) provider's servers or resources and the user are out of the United States; and (4) provider's servers or resources and the user are in the United States.[83]

The first, most common, scenario where the provider is based abroad but the user is within the United States will require the standard application done with similar electronic exports of technology or software. Essentially, if the user transmits controlled data to a cloud a standard export has occurred and the user must make sure that they comply with the EAR and undertake the proper process to receive a license for the product. With this scenario, the provider has no obligations to inform the user of potentially foreign locations of servers.

---

[80] BIS ADVISORY OPINION ON CLOUD COMPUTING, 992 PLI/Pat 982 (2011).

[81] Nixon Peabody, *The Export Control Implications of Cloud Computing*, 41 No. 17 THE LAWYER'S BRIEF 2.

[82] *Id.*; *see also* BIS ADVISORY OPINION ON CLOUD COMPUTING, 992 PLI/Pat 982 (2011).

[83] *US Export Controls and Cloud Computing*, LAW360, published September 10, 2010, available at http://www.law360.com (last visited Feb. 6, 2012); *see* BIS ADVISORY OPINION ON CLOUD COMPUTING, 984 PLI/Pat 985 (2009); BIS ADVISORY OPINION ON CLOUD COMPUTING, 992 PLI/Pat 982 (2011).

Second, another scenario may occur where the user is based abroad and the provider's servers are within the United States. Here, the guidelines by BIS become murky and we are forced to imply certain aspects of their opinions. Essentially, the 2009 AO clarified that providing a cloud service is not an activity subject to the EAR, but if that provider transmits controlled data to the user abroad, an export has occurred nonetheless. The provider, the BIS reasons, would not be responsible because they would not receive the "primary benefit . . . of the transaction," but who then will be responsible?[84] We may attempt to assume the BIS's meaning, but that would most likely be unfruitful with such a brief analysis on their part. In the end, this scenario shows BIS acknowledging that the EAR does not yet address how to deal with this situation.

Extending from the second scenario, a similar situation may arise if both the provider and the users are outside of the United States but dealing with U.S.-origin software or technology. For example, this issue may occur if a user, based in Turkey, decided to store data created within the United States in a cloud based in Scotland. In other words, this deals with the issue of re-exports.[85] The issue from the previous scenario comes back into play here. The BIS fails to address who would be responsible for this when dealing within the framework of cloud computing. Some analysts of the Advisory Opinions point to this also hinting at the lack of responsibility the provider in this situation would hold.[86]

Under the fourth scenario, the provider and the user are both within the United States, but the data or product is considered a "deemed export" because a foreign national has obtained it

---

[84] BIS ADVISORY OPINION ON CLOUD COMPUTING, 984 PLI/Pat 985 (2009).

[85] *US Export Controls and Cloud Computing*, LAW360, published September 10, 2010, available at http://www.law360.com (last visited Feb. 6, 2012) (U.S. origin product or data exported from one foreign country to another).

[86] *Id.*

from the provider. For example, if a U.S. based company uploads their product onto a cloud, such as Google Apps, and from there the product is downloaded and used by a foreign national. A situation may also arise in this scenario, with the same result, where an IT professional for the provider uses the product and it will still be considered a deemed export. The BIS has clearly stated the onus will be on the user in this situation, and it will be its responsibility to comply with the U.S. export control laws.[87]

With all the varying regulations forced upon the user, and the user alone, to comply with the export laws, cloud computing creates a huge potential for individuals and companies alike to inadvertently violate export control laws. Companies and individuals may be able to protect themselves from these nuances in export control law, but the burden is great and uneven. In a comprehensive article by Alexandra Lpez-Casero, she sets forth seven methods for users to protect themselves with the BIS comments in mind: (1) have a good command of the regulatory regimes, export control classifications, and licensing requirements applicable to their data or product; (2) Understand and seek out what will happen to the data or product once it is in the cloud; (3) incorporate cloud computing into company-wide policy; (4) review the agreement with the provider; (5) agree with the provider for clouds in limited geographic regions; (6) limit cloud use to items not subject to EAR; and (7) make sure the provider has policies in use to prevent foreign IT administrators from using the data.[88]

[87] BIS ADVISORY OPINION ON CLOUD COMPUTING, 984 PLI/Pat 985 (2009).

[88] Nixon Peabody, *The Export Control Implications of Cloud Computing*, 41 No. 17 THE LAWYER'S BRIEF 2.

D. *Any Guidance from Outside the BIS?*

Simply put, no. No other agency has made any comment on the way in which to best regulate the emerging cloud technology. For example, even though the State Department's Directorate of Defense Trade Controls ("DDTC") and the Treasury Department's Office of Foreign Assets Controls ("OFAC") have regulatory functions over domestic exports[89], neither has provided any guidance.[90]

E. *Where to Go from Here?*

Though informative, these Advisory Opinions are only that: opinions. The BIS does not speak for any other organization that controls U.S. exports, and therefore the law is still murky and in flux. Though the compliance methods laid out by Alexandra Lpez-Casero will help in the prevention of potential export control violations, it is only a temporary solution. Therefore, it is imperative that the government addresses cloud computing technology in an official manner through legislation. In fact, other governments, namely The United Kingdom and the European Union, took this step and have begun looking at how to handle these tangled and complicated issues. It would be quite informative to analyze their law as well as the style in which they enacted it.

IV. THE EUROPEAN MODEL FOR EXPORT LAW AND CLOUD COMPUTING

Without significant reform since the passing of EAA of 1979, the U.S. legislature needs to update their export control laws to properly reflect the changing climate of exportation. Though the United States has yet to make this significant step, other governments have begun the

---

[89] Nixon Peabody, *The Export Control Implications of Cloud Computing*, 41 No. 17 THE LAWYER'S BRIEF 2.

[90] *Id.*; Bowman, *supra* note 17 at 319, 334.

process with recent enactments attempting to clear the air and focus their laws on the changing marketplace.[91] In order for the United States to take the next step in regulating the exportation of technology through cloud computing, it would be greatly beneficial to see the style in which these foreign entities attempt to reign in the confusion swirling around cloud computer regulations. In this section, we will be reviewing and analyzing the export regulation of intangible items, such as those within cloud computing technology, in both the United Kingdom as well as within the larger European Union.

A. *United Kingdom's Export Control Act of 2002 and Its Effect on Cloud Computing*

After years of using an outdated act similar to the United States[92] that dated back to the export control theory "prevent trade with the enemy" (regarding Hitler and his rise to power), the United Kingdom passed the Export Control Act of 2002 ("EAC").[93] In the EAC, the United Kingdom defined an intangible export as the transfer of "software or technology by fax, telephone or other electronic devise."[94] In this context, the EAC defines a technology transfer as "a transfer by any means (or combination of means), including oral communication and the transfer of goods on which the technology is recorded or from which it can be derived."[95] Before

---

[91] *See* Export Control Act, 2002, c. 28 (Eng.), available at http://www.hmso.gov/acts/acts2002/20028--a.htm.

[92] *See* Import, Export, and Customs Powers (Defense) Act, 2 & 3 Geo. 6, c. 69 § (9)(3) (Eng.).

[93] Export Control Act, 2002, c. 28 (Eng.), available at http://www.hmso.gov/acts/acts2002/20028--a.htm; Bryan R. Reed, *The United Kingdom's New Export Control Act of 2002 and its Possible Impact on United Kingdom Universities and Academic Freedom: A Comparison of Export Control in the United States and the United Kingdom*, 8 UCLA J. INT'L & FOREIGN AFF. 193, 216.

[94] 8 UCLA J. INT'L & FOREIGN AFF. 193, 216; *see* The Dual-Use Items (export Control) Regulations (2000) SI 200/2620, available at http://www.hmso.gov.uk/si/si2000/20002620.htm (last visited Feb. 6, 2012).

[95] Export Control Act, 2002, c. 28 (Eng.), available at http://www.hmso.gov/acts/acts2002/20028--a.htm (last visited Feb. 6, 2012); Reed, *supra* note 94, at 216.

the EAC, the United Kingdom has not attempted to restrict technology transfers as exports,[96] but the enacting of this act pushed them into the forefront of technological export control. However, even with slight amendments to the act as recent as 2008,[97] the United Kingdom seems to be similarly behind on the cloud computing technology boom that has occurred throughout the world.

As stated by within a research paper by members within the United Kingdom government, there were two main purposes for the implementation of new export control laws: "(1) to strict the negative impact of arms trade and (2) to provide a transparent framework for legitimate exporters."[98] In fact, the government sought to "impose controls on the transfer of technology from the U.K. and by U.K. persons anywhere and by any means."[99] This ability to impose controls on technology within the United Kingdom is larger than one may first think because the government cast a wide net by defining technology within this act as "information . . . capable of use in connection with . . . an activity of any other kind whatsoever."[100] By defining technology so widely the EAC seems to give the government a wide discretion on whether to deem a move in the clouds as an export and the haze still swirls around the United Kingdom

---

[96] Reed, *supra* note 93, at 218.

[97] Underbill from 2008, 2006.

[98] Mark Oakes & Tim Youngs, Int'l Affairs and Defense Section, Research Paper 01/64, *The Export Control Bill of 2001-02*, at 3 (2001) available at http://www.parliament.uk/commons/lib/research/rp2001/rp01-064.pdf (last visited Feb. 6, 2012).

[99] *Id.*; 8 UCLA J. INT'L & FOREIGN AFF. 193 FOOTNOTE ("Among other powers listed are the power to: impose controls on technical assistance overseas, apply measures to 'give effect to EU legislation on controls of dual-use items,' initiate new licensing procedures . . . .").

[100] 8 UCLA J. INT'L & FOREIGN AFF. 193, 229; 631 Parl. Deb., H.L. (5th ser.) (2002) (statement of Baroness Miller of Hendon).

without any guideposts. However, the United Kingdom attempted to make the proper step forward by addressing the issue of intangible goods and the effect outdated tangible export control laws have on them. Unfortunately, they too seemingly have fell short on a concise proper control and this leaves the exportation of intangible items on cloud technology vague to say the least.

Though the EAC created an act similar to the EAA of 1979 (after multiple revisions since the EAA of 1979's enactment), the way in which the EAC arrived at the composition and content of the act are worth noting. The system by which they created this act occurred through the submission of Green Papers[101] and White Papers[102] by the United Kingdom government to create the best law for their people.[103] In this particular case, the government released both types of Papers in order to open a debate for the proper way to regulate the transfer of technology.[104] Specifically, the White Paper proposed wide regulations on the transfer of technology and the Green Paper pushed for new controls due to the danger of absolutely no control on the transfer of technology (a situation, luckily, the United States does not find itself in).[105] From that point, the government had an open dialogue with the public and within the legislature. In effect, the government went through a transparent process to create what they believed to be the best law by

[101] A Green Paper is a statement that is designed to stimulate discussion amongst a wide audience; http://www.historylearningsite.co.uk/how_laws_are_made_in_great_brita.htm (last visited Feb. 6, 2012).

[102] A White Paper is a statement of where the government wishes to go in the sense that it is fairly definite in what it thinks is required. http://www.historylearningsite.co.uk/how_laws_are_made_in_great_brita.htm (last visited Feb. 6, 2012).

[103] Reed, *supra* note 93, at 220.

[104] *Id.*

[105] *Id.*; *see also* Consultative Document on Strategic Export Controls, 1996 Cm. 3349; White Paper on Strategic Export Controls, 1998, Cm. 3989, available at http://www.dti.gov.uk/export.control/policy/whitepaper/index.htm (last visited Feb. 6, 2012).

allowing the experts within different fields to weigh in on the affect the act would have on the United Kingdom and abroad.

Another interesting facet to the EAC that the United States does not have within its export control laws is judicial review. In the United Kingdom system of export control the Secretary of State makes all final decisions on whether goods, intangible or tangible, will be considered for regulation.[106] The decision of the Secretary of State however, is subject to the scrutiny of the court system and must pass a balancing test to show he or she has not reached beyond the allotted power to control reasonably exported goods.[107] This balancing test is comprised of four steps: (1) Whether the Secretary has taken all relevant facts and other circumstances into account and dismissed all irrelevant facts; (2) whether the Secretary has identified all apparent interferences and the reasoning behind them; (3) whether the Secretary has considered the justifications for the degree of interferences; and (4) whether the Secretary balanced these justifications and the degree of control against the need to respect the freedom to carry out the identified activity.[108]

Though flawed in its own right, the EAC is important for us to be aware of it and to understand how it was created. By looking into the EAC and seeing the process of how it was formed, the U.S. legislature would have the potential to learn new and informative ways to approach U.S. export control laws that may not have been considered previously. The two approaches of note from the EAC are: (1) the use of the Green Paper and White Paper system; and (2) the introduction of Judicial Review into the process.

---

[106] Export Control Act, 2002, c. 28 §8 (Eng.), available at http://www.hmso.gov/acts/acts2002/20028--a.htm (last visited Feb. 6, 2012).

[107] *Id.*

[108] *Id.*

B. *European Union's Regulation 428/2009 and the Green Paper on Dual-Use Controls*

With the advent of technology in the world of exports, the countries within the European Union ("EU"), or "member states," had a fractured system without any real consistency. In fact, there is no explicit regulation of general cloud computing on a Europe-wide scale.[109] However, there are regulations similar in nature to the exportation of data through cloud computing that would help understand the climate of the European Union and would allow us to garner some incites in our own export control regulations regarding the movement of controlled technology on cloud computing technology.

The closest regulation the European Union has to regulation on exportation through cloud computing can be seen in its recent dual-use[110] exportation legislation. The current dual-use export control guidelines may be found in European Union Regulation 428/2009, but the rules within this are extremely complex and the regulation resultantly varies across the member states.[111] Due to this, on June 30, 2011, the EU Commission (hereinafter "the Commission")[112] released a Green Paper, similar to the aforementioned one in the United Kingdom, discussing the European Union's export control regulations for dual-use items and imploring the public to enter

[109] Jason P. Sluijs, Pierre Larouche & Wolf Sauter, *Cloud Computing in the EU Sphere,* TILEC Discussion Paper, Http://ssrn.com/abstract=1909877 (last visited Jan. 13, 2012).

[110] *Council Regulation (EC) No 428/2009*, OFFICIAL JOURNAL OF THE EUROPEAN UNION ch.1 art.2 (defined dual-use as "items, including software and technology, which can be used for both civil and military purposes").

[111] *Council Regulation (EC) No 428/2009*, OFFICIAL JOURNAL OF THE EUROPEAN UNION; Jacques Bourgeois, *European and Transatlantic Export Controls: Europe's New Dual-Use Green Paper* (2011) (last visited Feb. 6, 2012), available at http://www.wilmerhale.com/publications/whPubsDetail.aspx?publication=9901.

[112] The executive body of the European Union that is responsible for proposing and creating legislation as well as running the daily operations of the Union, available at http://ec.europa.eu/index_en.htm.

a debate about the proper way of regulating technology exportation.[113] This release of the Green Paper was done in an effort to create new consistent Europe wide regulations.[114]

The Commission focused on six major areas of potential improvement on the system currently in place[115]: (1) the creation of a "common risk assessment" between the member states; (2) increasing the exchange of information between member states; (3) Extending the scope of the European Union's Export authorization; (4) a catch-all control; (5) an integrated internal market for dual-use items; and (6) coordinated enforcement of export control rules.[116]

The actual intent of the Commission, though important in some respects, does not directly apply to the implementation of better U.S. exportation control on technologies. However, the overarching theme presented speaks directly to the issues presenting themselves within the United States. Specifically, the issues regarding the fractured nature of our system and how our regulations are vague and unhelpful to users can be seen in both the European Union and the United States. In fact, simply replace the term "member states," and enter "federal agencies" and one can see the similarity plainly.

The European Union took the next logical step, which the Unites States has yet to fully make, and admitted the system is a broken one and attempted to start the process of a significant overhaul. Once the United States can do that, they will be able to make strides in making an

---

[113] EU Green Paper: *The dual-use export control system of the European Union: ensuring security and competitiveness in a changing world* Brussels, 30.6.2011 COM (2011) 393 final.

[114] Peter Flanagan et al., *Recent Developments in EU Export Controls: EU Green Paper on Dual-use Exports*, EUROWATCH (Oct. 15, 2011), http://www.cov.com/publications/.

[115] *See id.*; Jacques Bourgeois et al., *European and Transatlantic Export Controls: Europe's New Dual-Use Green Paper* (July 28, 2011) http://www.wilmerhale.com/pages/publicationsandNewsDetail.aspx?NewsPubId=91593.

[116] Peter Flanagan et al., *Recent Developments in EU Export Controls: EU Green Paper on Dual-use Exports*, EUROWATCH (Oct. 15, 2011), http://www.cov.com/publications/.

efficient, fair system that regulates the exportation of intangible technology. There are too many agencies regulating exportation and an astounding lack of both communication and harmonious regulations. This has created a great deal of confusion, especially with a new system of exportation such as cloud computing.

In addition, the Commission is not doing this overhaul behind closed doors, but openly with the submission of a Green Paper to the public for its consideration. By opening the process to any willing member of the public, namely experts and businesspeople in the fields affected, the Commission has an opportunity to hear from those that know the most about how the legislation should be written and what it should include to make it better for the European Union as a whole.

V. RECOMMENDATIONS FOR THE FUTURE OF U.S. EXPORT CONTROLS ON CLOUD COMPUTING

In order to fix the U.S. export regulation system we must do more than tinker with it. In fact, the correction of our export control system calls for a complete overhaul. This statement is no truer than when discussing the particular export control regulation of intangible items. Specifically, those being exported through cloud computing. To fix the system we must: (1) consolidate the governmental regulation of U.S. export; (2) create a dual accountability system between user and provider; and (3) open up the export control legislation to the public and incorporate them into the creation of the regulations.

There needs to be a consolidation of U.S. export control laws. Currently, there are multiple agencies that regulate the export of intangible technology, and each has different regulations on certain items. With numerous agencies seemingly regulating the same items, only confusion can be created in the marketplace. This confusion will inevitably lead to a chilling

effect on one of the largest growing areas of the economy.[117] Similar to the Commission's Green Paper, where they suggested the creation of Europe-wide export control regulations, the United States needs to bring all the agency regulations into one universal regulation. This unification and synchronization will better allow for the U.S. market to grow and match the rest of the world economy.

An example may be seen just how bad it is in the United States through the AO 2009 and AO 2011 opinions. The BIS, only one organization of many, released an "opinion" on the effects of the EAR export control regulations on intangible items within cloud computing. This non-binding opinion answered few questions and left many doors open. Namely, the issue of every other agency that regulates exportations and how they would deal with cloud computing (frankly, including the BIS itself because of the opinions' non-binding nature). Without clarification on the state of export law on intangible items in clouds, the market will move elsewhere.

As the current system works, the user has the sole burden of making sure every facet of the provider's operations are in compliance with the regulations of U.S. export control law. From the location of the provider's servers to the nationality of its employees and even the safeguards it has if it does in fact have foreign national employees that may cause a deemed export risk. In this scenario, it seems the U.S. government has let the provider go scot-free. This is an unacceptable practice. In order for the system to work properly there must be explicit accountability from all sides of the operation, be it user or provider. With dual accountability, each side of the operation will be upfront with their operations and, in turn, this will cause less confusion and fewer violations.

---

[117] *See* Tim Weber, *Cloud Computing Goes Mainstream*, BBC NEWS (May 5, 2010) http://www.bbc.co.uk/news/10097450.

Following the lead from the United Kingdom and the European Union, the United States should open the process up to the public, namely those experts in the fields that know the best about the needs of the technology marketplace. By doing this, the U.S. legislature will be able to facilitate a conversation to foster the best form of regulation regarding cloud computing would make it transparent and allow for the proper regulations to be created in order for the market to grow without restrain or confusion. Though the legislature may be able to create a standard of regulation that would be workable to a layperson, the ability to take a sample from the experts in the field would ensure a viable law with real world applications. In essence, it will remove the chilling effect that the uncertainty from the current law creates within a technology field that is just beginning to understand cloud computing and what it may do for business.[118]

With these three areas addressed, the U.S. export control regulations would be a much more efficient and transparent system. Further, the use of cloud computing would have the opportunity it needs to grow into the market it is projected to be.

CONCLUSION

This Note argues that the United States export control regulations are outdated and in need of reform, particularly in regards to technology. Applying the United Kingdom's approach, the European Union's intent and the analysis of the 2009 and 2011 AOs, this Note believes a better and more efficient system is possible.

This Note acknowledges that the United States has begun considering reform of its export control system. This reform effort may potentially address the creation of a single export licensing authority, single enforcement agency, single control list, and single information

[118] *See* Cloud Computing Goes Mainstream by Tim Weber, http://www.bbc.co.uk/news/10097450 (Last visited Feb. 7, 2012).

technology system.[119] As part of this effort, the United States recently has introduced new export license exceptions, new control categories, and given guidance on issues such as the handling of disclosures of controlled technologies to dual nationals.[120] However, organizing the export control regulations in the United States, especially regarding cloud computing, seems to be far from a reality.

[119] WilmerHale, *European and Transatlantic Export Controls: Europe's New Dual-Use Green Paper*, available at http://www.wilmerhale.com/publications/whPubsDetail.aspx?publication=9901 (last visited Feb 7, 2012).

[120] *Id.*