NOTE

Clicking the "Export" Button: Cloud Data Storage and U.S. Dual-Use Export Controls

*Joseph A. Schoorl**

ABSTRACT

Use of online data storage services known generally as "cloud computing" could lead to unintentional violations of the United States' dual-use export control regime, the Export Administration Regulations ("EAR"). Transmission of data to servers outside of the United States constitutes an export under the EAR. Depending on the nature of the data transmitted and the location of the foreign server, the users of these cloud services could be liable for violations of the EAR. This Note argues that the EAR's fundamental reliance on the geographic destination of exports should not apply to the regulation of cloud computing. This regime threatens to undermine the development of an important technology without addressing the real threats that arise when U.S. companies store sensitive technical data on cloud servers. To remedy these failures, the Department of Commerce's Bureau of Industry and Security should create a new license exception for the storage of technical data on the cloud. This license exception would make the physical location of the cloud computing server irrelevant for purposes of the EAR and ensure that export-controlled technical data stored on the cloud is secure and protected.

* J.D., expected May 2012, The George Washington University Law School; B.A., 2009, University of California, Berkeley. For their assistance in this Note's production, I am extremely grateful to Brian Thavarajah, Alexander Hastings, Alexandre Lamy, Lauren Miller, and the entire staff of *The George Washington Law Review*. For their unwavering support through this and every other endeavor, I thank my parents, Andy and Cindy Schoorl; my sister, Katie; and all of my friends.

February 2012 Vol. 80 No. 2

Table of Contents

INTRODUCTION

Consumers are turning in increasing numbers to webmail and other Internet-based tools to solve communications and data storage problems.[1] The attraction of these services is simple: e-mail messages or files are stored on remote servers and accessed over the Internet so that the user is only a few clicks and a password away from her data no matter what computer she uses. If any of her computers sustain physical damage or become infected with malware,[2] data stored online remain intact and secure.[3] The physical location of this information—that is, the multiple servers that connect to the Internet and store user data—is irrelevant to the consumer who knows that access is available through any computer with an Internet connection. Indeed, it is unclear which discovery might be more surprising to the average webmail user: that the message she is reading on her screen could be stored on the other side of the world, or that this fact should even matter.

These conveniences and other factors are driving large corporations and small start-ups to consider utilizing similar web-based alternatives—generally labeled "cloud computing"—to solve mounting information technology problems.[4] The economic advantages of this approach can be particularly attractive: rather than purchase expensive hardware and pay growing legions of Information Technology ("IT") professionals to operate and maintain these systems for possi-

[1] For instance, according to one 2010 survey, more than seventy percent of respondents predicted that, within a decade, Internet-based applications would replace software running on a general purpose computer. *See* JANNA QUITNEY ANDERSON & LEE RAINIE, PEW INTERNET & AM. LIFE PROJECT, THE FUTURE OF CLOUD COMPUTING 8 (2010), *available at* http://www.pewinternet.org/~/media//Files/Reports/2010/PIP_Future_of_the_Internet_cloud_computing.pdf.

[2] Malware is "[m]alicious software . . . inserted into an information system to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners." Robert W. Ludwig, Jr. et al., *Malware and Fraudulent Electronic Funds Transfers: Who Bears the Loss?*, 16 FIDELITY L.J. 101, 103 (2010) (internal quotation mark omitted).

[3] Even when there is a technical glitch on the cloud, providers go to great lengths to protect data. On February 27, 2011, a small fraction of users of Google's Gmail webmail service found that all their data were unavailable. *See* Ben Treynor, *Gmail Back Soon for Everyone*, OFFICIAL GMAIL BLOG (Feb. 28, 2011), http://gmailblog.blogspot.com/2011/02/gmail-back-soon-for-everyone.html. Even though the glitch had affected multiple copies and multiple data centers, the information was still available on a tape backup and restored within a day. *See id.*

[4] One recent survey found that seventy-four percent of businesses used some sort of cloud computing service. *See* AVANADE, GLOBAL SURVEY: HAS CLOUD COMPUTING MATURED? 2 (2011), *available at* http://www.avanade.com/Documents/Research%20and%20Insights/FY11_Cloud_Exec_Summary.pdf. Furthermore, only one-fourth of the remaining twenty-six percent did not plan on eventually incorporating cloud computing into their businesses. *See id.*

ble future needs, corporations can simply purchase data storage or processing power as required.[5] Corporations pay a lower price for such resources because cloud providers can achieve greater efficiency through centralization and economies of scale.[6]

These conveniences and efficiencies encourage corporations to let their IT departments float into the clouds; various regulatory concerns, however, anchor these functions to the ground. The cloud is essentially a vast network of large computers called servers, which can be located anywhere an Internet connection is available.[7] Information is automatically allocated to different servers based on a number of factors, and these allocations generally occur without the knowledge of providers or users.[8] Due to the cloud's unique characteristics, transactions between cloud computing providers and users are subject to new and complex regulatory questions, including those related to the U.S. export control regime.

Questions about cloud computing and the Export Administration Regulations ("EAR"), which regulate items with dual military and commercial purposes as well as information about such items,[9] are currently too complicated to navigate confidently, and too serious to ignore. For example, imagine a company that designs and manufactures industrial chemicals, some of which could be used to produce toxic chemical agents. These chemicals, because they have both commercial and military purposes, are considered dual-use items and are regulated under the EAR.[10] The company would need to procure a license from the Commerce Department's Bureau of Industry and Security ("BIS"), the agency responsible for administering these regulations, to send either the chemicals or any information (e.g., formulae,

[5] *See* Michael Hugos & Derek Hulitzky, Business in the Cloud 30 (2011) (arguing that cloud computing will play an integral role in achieving the "business agility" that the modern economy necessitates).

[6] *See* Ludwig Siegele, *Let It Rise: A Special Report on Corporate IT*, Economist, Oct. 23, 2010, at 3–4; Rajen Sheth, *Disaster Recovery by Google*, Official Google Enterprise Blog (Mar. 4, 2010), http://googleenterprise.blogspot.com/2010/03/disaster-recovery-by-google.html (noting that Google can offer backup services much cheaper than private companies can because Google "operate[s] many large data centers simultaneously for millions of users, which helps reduce cost while increasing resiliency and redundancy").

[7] *See* Siegele, *supra* note 6, at 6–7.

[8] *See infra* notes 92–94 and accompanying text.

[9] Export Administration Regulations, 15 C.F.R. pts. 730–774 (2011). For information about the scope of the EAR, see *infra* Part I.A.

[10] Specifically, these chemicals are controlled under Export Control Classification Number ("ECCN") 1C350. 15 C.F.R. pt. 774, supp. 1.

production techniques, directions for use) about the chemicals to almost any nation outside of Europe.[11]

Similarly, if this manufacturer decided to store all its data using a cloud service and the cloud provider maintained servers in Mexico, the transmission of chemical-related information to that server would constitute an export requiring a BIS license.[12] It is unlikely that a license for this "export" would be obtained, however, because neither the cloud user nor the provider would be aware of the time and destination of such a transmission.[13] Nevertheless, failure to obtain a license could result in a violation of the EAR and fines of up to twice the value of the transaction or $250,000 *per transmission*.[14]

BIS has failed to address questions of how a cloud user's exports will be regulated. Since 2009, BIS has released two advisory opinions regarding the liability of cloud providers.[15] Neither opinion formulates a clear policy on what cloud computing users must do to comply with the EAR.[16] Though a BIS policy analyst reportedly stated that BIS was considering the problem of users storing data in a different country but only accessing it domestically,[17] no further action has been taken.

Some customers have negotiated terms requiring that all data be kept within the United States,[18] and commentators have suggested

[11] There is a general license requirement for exports of technologies classified under ECCN 1E350 to much of the world. *See id.* pt. 738, supp. 1. For more about the scope of the EAR, see *infra* Part I.A. For more about licensing requirements, see *infra* Part I.D.

[12] *See infra* text accompanying notes 96–97.

[13] *See infra* text accompanying notes 109–10.

[14] Export violators can also face criminal charges or the loss of export privileges. *See infra* notes 66–67, 69 and accompanying text.

[15] *See* Letter from C. Randall Pratt, Dir., Bureau of Indus. & Sec., Office of Nat'l Sec. & Tech. Transfer Controls (Jan. 11, 2011) [hereinafter 2011 Advisory Opinion], *available at* http://www.bis.doc.gov/policiesandregulations/advisoryopinions/jan11_2011.pdf (advisory opinion); Letter from C. Randall Pratt, Dir., Bureau of Indus. & Sec., Office of Nat'l Sec. & Tech. Transfer Controls (Jan. 13, 2009) [hereinafter 2009 Advisory Opinion], *available at* http://www.bis.doc.gov/policiesandregulations/advisoryopinions/jan13_2009_ao_on_cloud_grid_computing.pdf (advisory opinion).

[16] As practitioner and blogger Clif Burns noted after BIS issued the 2011 advisory opinion, "[N]one of this addresses the 900-pound gorilla in the room which is, of course, the user of the cloud service." Clif Burns, *Once More unto the Breach*, EXPORTLAWBLOG (Feb. 8, 2011, 8:35 PM), http://www.exportlawblog.com/archives/2844.

[17] *Cloud Computing Provides Unique Export Control Challenges*, INSIDE U.S. TRADE, Jan. 7, 2011, at 13.

[18] Patrick Thibodeau, *Microsoft's Cloud-Enabled Office 2010 Set to Join Battle with Google: Contract Terms, Not Features, May Have Major Role in Google Apps vs. Office Cloud Decisions*, COMPUTERWORLD (Apr. 8, 2010, 7:05 AM), http://www.computerworld.com/s/article/9175019/Microsoft_s_cloud_enabled_Office_2010_set_to_join_battle_with_Google (re-

that cloud providers allow customers to pay a premium to exert control over the location of their data.[19] These approaches are both unsustainable and unwise. First, these solutions are likely not available to smaller users who lack a strong bargaining position. Second, such limitations could have adverse effects on the development of cloud technologies and business models. As one commentator notes, "[t]he fluidity of the flow of data and the variety of location of computers and servers are inherent to the cloud concept."[20] Adding additional U.S. regulatory burdens could distort the market by affecting investments in cloud infrastructure. Finally, cloud users could never be certain that cloud providers would not inadvertently or intentionally violate agreements to retain information in a specific geographic location.[21]

Undermining the growth of cloud computing is a high price to pay, especially when weighed against the limited national security gains.[22] Export controls, particularly on dual-use items, depend on a complex formula designed to assess what actors in specific countries might do with access to sensitive goods and technologies.[23] Yet, just as the location of a server is irrelevant to the user of a webmail service, the location of data on a server in, say, Russia does not make it more accessible to Russian individuals.[24] And just as the cloud can be accessed through any Internet-enabled computer, it can also be hacked into from anywhere.[25] Cloud computing was designed to decouple access from location in a way that fundamentally undermines the basic assumptions of the U.S. export control regime.

This Note proposes a modest step toward realigning the application of export controls with the diminished and distinguishable national security threats that accompany storing controlled data on the

porting that a term in the City of Los Angeles's cloud computing contract with Google required all data to remain within the continental United States).

[19] John Villasenor, Brookings Inst., Ctr. for Tech. Innovation, Addressing Export Control in the Age of Cloud Computing 7 (2011), *available at* http://www.brookings.edu/~/media/Files/rc/papers/2011/0725_cloud_computing_villasenor/0725_cloud_computing_villasenor.pdf.

[20] Francoise Gilbert, *Cloud Service Contracts May Be Fluffy: Selected Legal Issues to Consider Before Taking Off*, J. Internet L., Dec. 2010, at 1, 22.

[21] *See* Villasenor, *supra* note 19, at 8.

[22] *See id.* at 9 (noting that "tradeoffs at the intersection of cloud computing and export control are particularly nuanced" because overregulation could make American companies unable to fully benefit from the cloud's efficiencies and, thus, less able to compete globally).

[23] *See infra* text accompanying note 54.

[24] *See infra* text accompanying notes 112–13.

[25] Although this raises security concerns, they are very much distinguishable from those that the EAR are designed to address. *See infra* text accompanying notes 112–13.

cloud. This step would take the form of a license exception to the EAR for American cloud users storing information to be used domestically. Part I introduces the United States' current dual-use export control regime, specifically considering those aspects of the EAR that are most relevant to the analysis of cloud computing and the proposed solution. Part II provides an overview of cloud computing and explains one of the problematic ways that the EAR apply to this emerging technology. Part III proposes regulatory language for the licensing exception, explains its rationale, and provides examples of how cloud users could (and could not) use the exception. Finally, Part IV responds to possible counterarguments.

I. Overview of the Export Administration Regulations

The modern EAR can be traced to the Export Administration Act of 1979,[26] though both have undergone numerous changes in years since. The Act has expired and been renewed numerous times, but Congress has not renewed it since it lapsed in 2001.[27] Whenever the statute is in lapse, the President extends the EAR's applicability by executive order under the International Emergency Economic Powers Act.[28]

This Part considers five basic concepts of the EAR: (A) the scope of the EAR, (B) the definition of "exports," (C) the concept of "deemed exports," (D) licensing requirements and licensing exceptions, and (E) enforcement.

A. *Scope of the EAR*

The EAR regulate dual-use items, which are items with both military and commercial applications.[29] The regulations state that all items originating from or located in the United States can be "subject

[26] Export Administration Act of 1979, Pub. L. No. 96-72, 93 Stat. 503 (expired 1994). For more information on the history of export controls prior to the Act, see Antonia Alice Badway, Comment, *Controlling the Export of Dual-Use Technology in a Post-9/11 World*, 18 Transnat'l Law. 431, 434–40 (2005).

[27] *See* Badway, *supra* note 26, at 437 (noting that the Act expired in August 2001).

[28] International Emergency Economic Powers Act, 50 U.S.C. §§ 1701–1707 (2006). For the most recent extension of the Export Administration Act, see Continuation of Emergency Regarding Export Control Regulations, 76 Fed. Reg. 50,661 (Aug. 16, 2011).

[29] 15 C.F.R. § 730.3 (2011). The Department of State regulates items designed solely for military purposes under the International Traffic in Arms Regulations, 22 C.F.R. pts. 120–130 (2011). The Department of Energy, the Department of the Treasury, the Nuclear Regulatory Commission, and the Patent and Trademark Office also play limited roles in export controls. *See* 15 C.F.R. § 734.3(b)(1).

to the EAR."[30] This also includes foreign products that incorporate more than de minimis amounts of U.S. items, or that are the direct product of certain U.S.-origin technologies or software.[31]

In the EAR, the word "item" takes on a different meaning than in normal language: it includes commodities, technology, and software.[32] "Technology," the focus of this Note, is an especially amorphous term that includes the specific information necessary for the "development, production, or use of a product"[33] that is not publicly available.[34] This includes blueprints, engineering designs, product specifications, and even instruction manuals.[35]

B. Exports and Reexports

Though many goods and related technologies could be subject to the EAR, the regulations only apply to exports of these items. Like most terms in the EAR, however, the word "exports" includes considerably more than one might assume. "Exports" is defined as the "actual shipment *or transmission* of items subject to the EAR out of the United States."[36] If an exported item is shipped or transmitted from one foreign country to another, it qualifies as a "reexport."[37] In either of these cases, actual shipments would include what might be considered "traditional" exports involving the physical transfer of custody over an item from one party (American in the case of an export, foreign in the case of a reexport) to a second, foreign party.[38]

The word "transmission," however, dramatically expands the variety of transactions to which the EAR apply.[39] Though they do not specifically define "transmission," the regulations do state that "elec-

[30] 15 C.F.R. § 734.3(a)(1)–(2). The Export Administration Act granted regulatory authority over "any goods or technology subject to the jurisdiction of the United States or exported by any person subject to the jurisdiction of the United States," giving a clear indication of the statute's intended extraterritoriality. Export Administration Act of 1979 § 5(a)(1), 93 Stat. at 506, 513, 515.

[31] 15 C.F.R. § 734.3(a)(3)–(4).

[32] *Id.* § 772.1.

[33] *Id.* (internal quotation marks omitted). Each of these three terms is also defined. *Id.*

[34] *Id.* § 734.2(a)(1). The meaning of "publicly available technology" is addressed in 15 C.F.R. §§ 734.7–.11.

[35] *Id.* pt. 734, supp. 1. It also can include technical assistance, such as individuals training or instructing users of a product. *Id.* pt. 734, supp. 1, question C(6).

[36] *Id.* § 734.2(b)(1) (emphasis added).

[37] *Id.* § 734.2(b)(4).

[38] *Id.* § 734.2(b)(1), (4).

[39] *See* Berne C. Kluber, *Global Distributions: The Effect of Export Controls*, 23 HOUS. J. INT'L L. 429, 436–37 (2001) ("By using the word 'transmission' the government clearly intends that the use of electronic mail ('e-mail') or the Internet to send items be subject to the EAR.").

tronic transmission of non-public data" is an export.[40] A more extensive list of transmissions included elsewhere in the EAR makes this point especially clear.[41] Finally, such transmissions need not be made within the context of an economic transaction between two independent parties. An "export" also occurs when an American company sends information to a foreign branch or subsidiary.[42]

C. Deemed Exports

The expansive concept of exporting outlined above is even broader under the "deemed export" rule. BIS deems that an export occurs when there is a "release" of controlled technology to a foreign national, even if this occurs within the United States.[43] These exports are a legal fiction, based on the assumption that conveying information to a foreign national will result in the information being relayed to that national's home country.[44]

Such releases can occur in a number of different settings. They range from allowing a foreign national to inspect a product or technical data, to having a conversation with a foreign national.[45] However, the rule applies not only to actual releases, but also to possible releases: if a foreign employee can access a controlled commodity,

[40] 15 C.F.R. § 730.5(c).

[41] The EAR define the export of encryption source code to include

> downloading, or causing the downloading of, such software to locations (including electronic bulletin boards, Internet file transfer protocol, and World Wide Web sites) outside the U.S., or making such software available for transfer outside the United States, over wire, cable, radio, electromagnetic, photo optical, photoelectric or other comparable communications facilities accessible to persons outside the United States, including transfers from electronic bulletin boards, Internet file transfer protocol and World Wide Web sites.

Id. § 734.2(b)(9)(B)(ii).

[42] *See* Gregory W. Bowman, *E-mails, Servers, and Software: U.S. Export Controls for the Modern Era*, 35 Geo. J. Int'l L. 319, 337 (2004). BIS attempted to address this through License Exception Intra-Company Transfer, which would have reduced license requirements on items and technology that remained within the possession of the company. Establishment of License Exception Intra-Company Transfer (ICT), 73 Fed. Reg. 57,554, 57,559 (proposed Oct. 3, 2008) (to be codified at 15 C.F.R. pt. 740). However, BIS does not seem likely to finalize this license exception.

[43] *See* 15 C.F.R. § 734.2(b)(3).

[44] *Id.* § 734.2(b)(2)(ii). Licensing for deemed exports depends upon the nationality of the foreign national in question. For instance, release of technical data to a Czech citizen would be subject to the same licensing standards as an export of that technical data to the Czech Republic. *See* Benjamin H. Flowe, Jr., *Exporting Technology and Software, Particularly Encryption*, *in* Coping with U.S. Export Controls 2009, at 195, 211 (PLI Commercial Law & Practice, Course Handbook Ser. No. A-919, 2009).

[45] *See* 15 C.F.R. § 734.2(b)(3)(i)–(ii) (defining "release of technology" as "visual inspection" of equipment or "oral exchanges of information").

software, or technology, it could qualify as a deemed export regardless of whether the employee actually accessed the information.[46] In an age where company networks centralize employees and information, compliance with this rule has become especially tricky.[47]

D. *Licensing Requirements and License Exceptions*

If an item is subject to the EAR, and an export, reexport, or deemed export will occur, a license from BIS is not always necessary. After determining that a transaction involves items subject to the EAR and that an export will occur, exporters must identify whether the commodity, technology, or software is listed on the Commerce Control List ("CCL").[48] This is a list of specifications for dual-use items, and each entry is assigned an Export Control Classification Number ("ECCN").[49] If an item does not appear on this list, it is "EAR99," a catch-all classification.[50] EAR99 items require a license from BIS only in a small number of situations, such as when the destination is an embargoed nation or the item will be used for prohibited end-uses or by prohibited end-users.[51]

If the item appears on the CCL, exporters must use the list to find the item's "reason for control."[52] There are fourteen enumerated reasons for control, including Anti-Terrorism, Chemical and Biological Weapons, Missile Technology, and National Security.[53] On the Commerce Country Chart, each country is listed along with the applicable reasons for control.[54] Exporters must determine whether the item is controlled for reasons that apply to the destination country; if not,

[46] *See* Flowe, *supra* note 44, at 210.

[47] *See* Christopher F. Corr, *The Wall Still Stands! Complying with Export Controls on Technology Transfers in the Post-Cold War, Post-9/11 Era*, 25 HOUS. J. INT'L L. 441, 475 (2003) ("One area of particular difficulty concerns the increasing use of internal company email servers, or intranets, where proprietary data is shared among employees, and broad company computer networks where a foreign national may gain access to controlled data and files.").

[48] *See* Cecil Hunt, *Department of Commerce Export Controls*, *in* COPING WITH U.S. EXPORT CONTROLS 2009, *supra* note 44, at 89, 101.

[49] *Id.*

[50] *Id.*

[51] Bowman, *supra* note 42, at 340. These limitations on EAR99 items can be traced to the EAR's General Prohibitions Four through Ten. 15 C.F.R. § 736.2(b)(4)–(10) (2011). An "end-user" is a "person abroad that receives and ultimately uses the exported or reexported items," while an "end-use" is the way in which the end-user will use the item. *Id.* § 772.1. EAR99 items are not affected by cloud computing or the proposed Cloud Computing License Exception discussed in Part III, *infra*, and will therefore not be considered further.

[52] 15 C.F.R. § 772.1.

[53] *Id.*

[54] *See id.* pt. 738, supp. 1.

then there will be no additional licensing requirements beyond those that exist for an EAR99 item.[55]

If items are controlled for a reason that applies to the destination country, a license will generally be required unless there is a license exception.[56] License exceptions allow exports or reexports without a required license when certain conditions are met.[57] For instance, License Exception Civil End-Users allows the export of some items that are controlled only for National Security reasons if the items are "destined for civil end-users for civil end-uses."[58] Importantly, all of the existing license exceptions require the exporter to identify each exported item and each destination country.[59]

As an example of this process, imagine a U.S. company trying to export integrated circuits with a total value of $4000 to Mexico. After consulting the CCL, the company's attorney determines that, because the circuits are "storage integrated circuits manufactured from a compound semiconductor," they fall under ECCN 3A001.a.4.[60] These circuits, according to the CCL, are controlled for National Security and Anti-Terrorism reasons.[61] The attorney then consults the Commerce Country Chart, where he notes that items controlled for National Security reasons require a license for export to Mexico.[62] However, the attorney notices on the CCL that License Exception Shipments of Limited Value is applicable for shipments of ECCN 3A001.a items with values less than $5000.[63] Because the shipment to Mexico is worth only $4000, and because this particular exception applies to shipments to Mexico, no license would be required to make this export.[64]

[55] *See* Hunt, *supra* note 48, at 102.

[56] *See* Bowman, *supra* note 42, at 340–41.

[57] *See* 15 C.F.R. § 740.1.

[58] *Id.* § 740.5(a).

[59] Bowman, *supra* note 42, at 341. This is also true of the recently finalized License Exception Strategic Trade Authorization ("License Exception STA"), which removes licensing requirements for different classes of destination countries. Export Control Reform Initiative: Strategic Trade Authorization License Exception, 76 Fed. Reg. 35,276, 35,287 (June 16, 2011) (to be codified at 15 C.F.R. pt. 740).

[60] 15 C.F.R. pt. 774, supp. 1.

[61] *See id.* pt. 738, supp. 1; *id.* pt. 774, supp. 1.

[62] *Id.* pt. 738, supp. 1. Anti-Terrorism is not a reason for control that is applicable to Mexico. *Id.*

[63] *Id.* pt. 774, supp. 1.

[64] *See id.* § 740.3 (stating that License Exception Shipments of Limited Value can be applied to Country Group B); *id.* pt. 740, supp. 1 (identifying Mexico as being in Country Group B).

E. Violations and Penalties

Failure to successfully navigate this complicated process can be costly. Exporting a controlled item without procuring a required license or having a valid license exception can result in civil or criminal penalties.[65] These penalties can be severe: civil violations are punishable with fines up to the greater of twice the value of the transaction or $250,000, whereas criminal violations can net fines of $1 million and twenty years in prison.[66] Besides monetary penalties, BIS can also restrict or deny civil violators from taking part in any export transactions for up to ten years.[67]

Another noteworthy aspect is the culpability required for violations. All criminal and most administrative violations of the EAR include a mens rea component. For instance, the regulations prohibit possession of an item with the *intent* to export or *knowledge* that the item will be exported in violation of the EAR.[68] However, some administrative penalties can be applied on a strict liability basis. One violation is "engaging in prohibited conduct," which can be found without any showing of culpability.[69] For example, if an exporter believes that the product did not require a license because it is EAR99, but in fact the item did appear on the CCL and required a license, civil charges can apply on a strict liability basis.[70]

II. Cloud Computing Under the EAR

This Note now turns to how the EAR apply to the more complicated question of cloud computing. This Part identifies the technological characteristics of the cloud computing model. It then shows that one of the most basic uses of the cloud, data storage, involves users in activities subject to the EAR that could require a practically unobtainable license. Finally, it considers the inherent problems in regulating cloud transmissions under the EAR.

[65] *See id.* § 764.3(a)–(b).

[66] *Id.* § 764.3(a)(1)(i), .3(b); *see also* International Emergency Economic Powers Enhancement Act, Pub. L. No. 110-96, sec. 2, § 206(b)–(c), 121 Stat. 1011, 1011 (2007).

[67] 15 C.F.R. § 764.3(a)(2).

[68] *Id.* § 764.2(f).

[69] *Id.* § 764.2(a); *see also* Iran Air v. Kugelman, 996 F.2d 1253, 1259 (D.C. Cir. 1993) ("[T]he language of the [Export Administration Act] and the [EAR] adequately indicated that civil sanctions could be assessed on a strict liability basis.").

[70] *See* Doreen Edelman, *Enforcement of Export Control Violations on the Rise*, Fed. Law., Oct. 2008, at 18, 18–19.

A. Introduction to Cloud Computing

The term "cloud computing" is notoriously difficult to define. The National Institute of Standards and Technology defines the phrase as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[71] Comparisons to previous models of computing can be more illustrative. Personal computer users have traditionally accessed software or data installed or stored on a computer that they or their employers owned. Now similar applications and features reside online.[72]

The types of services and applications available through cloud computing can differ vastly. Some services allow providers to host applications online "without the need for the customer to house and maintain the application in its own data center."[73] Google Docs is a simple example; it allows users to create and edit text documents, spreadsheets, and slideshows (functions traditionally performed using applications like Microsoft's Office Suite) entirely through a web browser.[74] Other services allow customers to develop applications using tools and infrastructure located on a provider's network.[75]

This Note's focus, though, is on "Infrastructure as a Service."[76] This resource allows customers to store data on a "cloud" and access it over the Internet.[77] For instance, the consumer product Dropbox allocates a certain amount of storage space to customers.[78] After users upload files through the Dropbox website or desktop application, the

[71] PETER MELL & TIMOTHY GRANCE, U.S. DEP'T OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., THE NIST DEFINITION OF CLOUD COMPUTING 2 (2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[72] HUGOS & HULITZKY, *supra* note 5, at 44.

[73] *Id.* These services are labeled under the general term "Software as a Service." *Id.* Because software is controlled under the EAR, providers of online-application services face a unique set of export-compliance challenges. For an excellent review of these challenges, see John F. McKenzie, *U.S. Export Controls on Internet Software Transactions*, 44 INT'L LAW. 857 (2010).

[74] *See* GOOGLE DOCS, http://docs.google.com (last visited Dec. 28, 2011). Other examples include Facebook, YouTube, and webmail services. Timothy D. Martin, *Hey! You! Get Off of My Cloud: Defining and Protecting the Metes and Bounds of Privacy, Security, and Property in Cloud Computing*, 92 J. PAT. & TRADEMARK OFF. SOC'Y 283, 287 (2010).

[75] HUGOS & HULITZKY, *supra* note 5, at 44. Generally, these services are classified as "Platform as a Service." *Id.*

[76] *Id.*

[77] *Id.*

[78] *See* DROPBOX, http://www.dropbox.com (last visited Dec. 28, 2011).

files are stored on Dropbox's servers and can be accessed on other computers or even mobile phones.[79] At any time, users can purchase more online storage space, which is billed on a monthly basis.[80] This basic model of "provid[ing] resizable compute capacity" exists throughout all cloud providers.[81]

The cloud itself is less ethereal than its name suggests: it is composed of many interconnected servers that are themselves just large concentrations of individual computers.[82] These servers can be located anywhere in the world with adequate electricity and Internet connectivity,[83] and providers prefer to conceal the location of their servers for competition and data security reasons.[84] Critically, companies purchasing these services are not purchasing a number of physical servers. Rather, they are purchasing a "virtual machine" that behaves like a physical computer but actually utilizes resources from numerous interconnected servers.[85] In this manner, multiple virtual machines can operate on a single server, and multiple servers can contribute resources to a single virtual machine.[86] This flexibility allows for dynamic scalability based on the consumer's needs.[87] These "disembodied" computers can also be created quickly, duplicated to serve as backups, and moved between servers while running.[88]

The upshot of this form of computing is that a user transforms his or her personal computer, which has dedicated but limited processing power and data storage space, into a modern "dumb terminal"[89] used

[79] *Features*, DROPBOX, http://www.dropbox.com/features (last visited Dec. 28, 2011).

[80] *Pricing*, DROPBOX, http://www.dropbox.com/pricing (last visited Dec. 28, 2011).

[81] *Amazon Elastic Compute Cloud (Amazon EC2)*, AMAZON WEB SERVICES, http://aws.amazon.com/ec2/ (last visited Dec. 28, 2011). Amazon's Elastic Cloud Compute, a service that targets businesses rather than consumers, allows customers to "automatically scale . . . capacity up or down according to conditions" that the user defines. *Id.*

[82] *See* Siegele, *supra* note 6, at 6.

[83] *Id.*

[84] *See* Peter Fleischer, *The Cloud: Policy Consequences for Privacy when Data No Longer Has a Clear Location*, PETER FLEISCHER: PRIVACY . . . ? (Apr. 16, 2009, 9:53 AM), http://peterfleischer.blogspot.com/2009/04/cloud-policy-consequences-for-privacy.html.

[85] HUGOS & HULITZKY, *supra* note 5, at 37. Users of Apple's Macintosh OS X might be familiar with virtualization if they use programs such as VM Fusion, which allows users to open a window in OS X that behaves like a desktop computer running a Windows or Linux operating system. *See VMware Fusion: Run Windows on Mac for Desktop Virtualization*, VMWARE, http://www.vmware.com/products/fusion/ (last visited Dec. 28, 2011).

[86] *See* Siegele, *supra* note 6, at 6.

[87] *See* Gilbert, *supra* note 20, at 18 (noting that cloud capabilities "can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out or in").

[88] Siegele, *supra* note 6, at 6.

[89] A dumb terminal is an "input/output device that is used for communication with a computer from a remote site," but that lacks the "built-in capability to store and manipulate data."

only to access the unlimited resources of the cloud.[90] Just as any computer with an Internet connection can be turned into a dumb terminal, so too can any server provide the processing power and data storage for the virtual machine that the dumb terminal is accessing.[91]

A number of considerations can compel the movement of a virtual machine between data centers. For instance, the network might need to shift computing work from busy servers to idle ones.[92] Providers also maintain copies of virtual machines on multiple servers to ensure that user data is not lost should a problem occur at any one data center.[93] As Google's global privacy counsel notes, these fundamental characteristics make it "actually very hard to answer the apparently simple question: 'where's my data?'"[94]

B. *Cloud Computing and the EAR*

The constantly shifting location of data in the cloud, combined with the global distribution of some providers' data centers, makes the cloud especially vexing from an export control standpoint. As mentioned above, all data necessary for the development, production, or use of a product and not publicly available are subject to the EAR.[95] If the originator of such data uses a basic cloud service for data storage or webmail, and that service uses a network of servers that extends beyond U.S. borders, then any transfer of data from the user to such a server constitutes a "transmission" and, thus, an export.[96] Given such a set of events, a violation of the EAR would hinge on the

THE FACTS ON FILE DICTIONARY OF COMPUTER SCIENCE 202 (Valerie Illingworth & John Daintith eds., 4th ed. 2001).

[90] William Jeremy Robison, Note, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1200 (2010).

[91] *See* Gilbert, *supra* note 20, at 18 (noting that both "ubiquitous network access"—the ability to access the data from any computer—and "resource pooling"—the ability to assign and reassign resources dynamically—are essential components of the cloud).

[92] Fleischer, *supra* note 84.

[93] *See* Sheth, *supra* note 6 ("[E]very action you take in Gmail is simultaneously replicated in two data centers at once . . . .").

[94] Fleischer, *supra* note 84. Obviously, this uncertainty about a data location extends to the cloud user. *See* Gilbert, *supra* note 20, at 18 ("[T]he customer generally has no control over, or knowledge of, the exact location of the resources . . . .").

[95] *See supra* notes 29–33 and accompanying text.

[96] An official from BIS reportedly confirmed this interpretation of the EAR at the 2010 BIS Update Conference. *Cloud Computing Provides Unique Export Control Challenges*, *supra* note 17, at 13. A transfer from one server in the United States to a non-U.S. server would be an export for which the user could be liable. *See supra* notes 40–42 and accompanying text. Moreover, a transfer between two non-U.S. servers would constitute a reexport that could also violate the EAR. *See supra* note 37 and accompanying text.

ECCN of the technical data and the country in which the server resides.[97]

An additional concern is that foreign national employees of the cloud provider could have access to a cloud user's controlled content. Depending on their nationality, this access would be a potential violation of the deemed export rule.[98] BIS has not clearly stated how the deemed export rule would apply in the cloud computing context, but it seems likely that the cloud user would be responsible for ensuring that there are no foreign nationals working for the chosen cloud provider.[99] In such cases, the nationality of the foreign employee would determine whether a violation occurred.[100]

Though it strains credulity to classify data transfers in these terms, restrictions on these activities are consistent with how the EAR have been applied to related activities. BIS has, for example, charged businesses with EAR violations that were committed by e-mailing data to an individual in another country.[101] Attorneys have also consistently warned clients that intranets and virtual private networks used by foreign employees in multinational companies to access controlled information could raise compliance concerns.[102]

Traditional examples of e-mail and network access are distinguishable from the typical cloud computing–compliance scenario because, in the former situation, the "exported" data is being accessed outside of the United States. That is, someone has to be in another country to open the e-mail or access the network. In a 2009 advisory opinion, however, BIS did not emphasize this difference; rather, the agency analyzed the problem in the traditional, location-based framework.[103] BIS issued this opinion in response to questions from an unidentified cloud computing provider and largely assuaged the export control concerns of this group: the only foreseeable liability would be

[97] *See supra* Part I.D.

[98] *See* VILLASENOR, *supra* note 19, at 6.

[99] *See id. But see* 2011 Advisory Opinion, *supra* note 15 (stating that cloud providers would generally not be responsible for foreign national IT personnel accessing controlled technical data).

[100] *See supra* Part I.C.

[101] *See* LogicaCMG, Inc. (Dep't of Commerce, Bureau of Indus. & Sec. May 4, 2007) (order), *available at* http://efoia.bis.doc.gov/exportcontrolviolations/e1067.pdf (charging company for, among other offenses, e-mailing technical data to Cuba in violation of a U.S. embargo).

[102] *See* Corr, *supra* note 47, at 523 (stressing that multinational companies must ensure that controlled data are not accessible from "overseas terminals" because this could constitute an export).

[103] 2009 Advisory Opinion, *supra* note 15, at 3–4. In its analysis, BIS considered the location of the server controlling. *Id.*

for shipping information not publicly available about how to use a cloud service and for knowingly assisting other parties in the development of missile technology.[104]

This advisory opinion did little to clarify the possible liability of cloud users.[105] Since the opinion's issuance, a BIS senior policy expert reportedly confirmed that the act of saving controlled data to an international server would constitute an export.[106] However, BIS has not yet made a formal decision about how to handle these exports.[107] Unsurprisingly, numerous practitioners have advised clients against using the cloud for any controlled technology.[108]

C. *Problems Related to Cloud Computing Under the EAR*

There are inherent problems with regulating free-flowing data through the destination-based EAR. It would be impossible for a company wishing to take advantage of cloud computing efficiencies to obtain a license for such activities. First, cloud providers, much less cloud users, are usually unaware of the location of data or the occurrence of transfers across national borders,[109] but this information would be essential for both obtaining a license or availing oneself of a license exception.[110] Second, because these regulatory concerns are ill defined and less than intuitive, cloud users may not even be aware of the export control implications—they might not know that they need

[104] *Id.* BIS based its interpretation on the fact that the cloud provider would not, in normal circumstances, qualify as an "exporter" as that term is defined in the EAR because it was not receiving the "primary benefit" of the shipment. *Id.* at 3 (citing 15 C.F.R. § 772.1 (2011)).

[105] *See* Clif Burns, *Cloudy with a Chance of Fines*, EXPORTLAWBLOG (Jan. 12, 2010, 9:23 PM), http://www.exportlawblog.com/archives/1187 (cautioning that the advisory opinion "fails to address the export issues relating to users of such cloud computing services"); Eric R. McClafferty, *Exporting into the Clouds: Export Compliance Issues Associated with Cloud Computing*, TMCNET.COM (Jan. 11, 2010), http://hosted-voip.tmcnet.com/feature/articles/72410-exporting-into-clouds-export-compliance-issues-associated-with.htm (noting that the 2009 advisory opinion "makes it clear that the transfer of software or technology that is subject to the regulations remains controlled for export").

[106] *Cloud Computing Provides Unique Export Control Challenges*, *supra* note 17, at 13.

[107] *Id.* (reporting that the official explained that BIS is "looking into the aspect of access because many of you are storing data in a different country, but it's only accessed by your company [sic] individuals in the United States").

[108] *See, e.g.*, Brian P. Curran, *US Export Controls and Cloud Computing*, LAW360 (Sep. 10, 2010), http://www.law360.com/articles/192649/us-export-controls-and-cloud-computing ("[C]loud users and providers must do their best to apply traditional rules regarding software and technology transfers to the world of cloud computing."); McClafferty, *supra* note 105 (urging companies to consult counsel if they are considering using cloud computing or have done so and violated the EAR).

[109] *See supra* notes 92–94 and accompanying text.

[110] *See supra* note 59 and accompanying text.

an unobtainable license. This lack of knowledge, though, would not shield them from export control violations and penalties because of the EAR's strict liability provisions.[111]

The focus on the physical location of data also fails to address the real data security concerns raised by the use of cloud computing. The political characteristics or military ambitions of the country where the server is located do not correlate with threats to the physical security of servers[112] or the network's overall vulnerability to hackers.[113] Therefore, the licensing requirement would do little to distinguish between dangerous and safe uses of foreign servers as part of a cloud network.

Moreover, this location-based regime does little to ensure that the entire network is protected from unauthorized access. In contrast to the broad control afforded to users of private networks, cloud users normally have little control over the security measures that protect their data from outsiders after making their initial decision between cloud providers.[114] Concerns continue to grow about other countries targeting private U.S. cloud computing networks to steal secret military information[115] because the concentration of data on those clouds makes them enticing targets.[116] It is also conceivable that foreign governments, through regulatory or subpoena pressure, could gain access to private user data found in data centers in their jurisdictions.[117] The current EAR do not address any of these concerns.

[111] *See supra* note 69 and accompanying text.

[112] Each cloud provider has its own policy on securing its servers from physical intrusions. *See, e.g.*, Google Apps, *Google Data Center Security*, YOUTUBE (Apr. 13, 2011), http://www.youtube.com/watch?v=1SCZzgfdTBo (highlighting Google's use of security features such as perimeter fences, 24/7 security presence, access control, and video surveillance in their server farms).

[113] *But see* 15 C.F.R. § 730.6 (2011) (noting that a purpose of export controls is "to restrict access to dual-use items by countries or persons that might apply such items to uses inimical to U.S. interests").

[114] *See Cloudy with a Chance of Rain*, ECONOMIST: TECH.VIEW (Mar. 5, 2011), http://www.economist.com/node/15640793?story_id=15640793.

[115] For instance, a former presidential adviser on cyber security stated that there was "good reason to believe" that China or another foreign government hacked into a corporate network to download plans for the next generation F-35 fighter jet. Robert Keating, *The Cyber Warrior*, DISCOVER, July/Aug. 2010, at 58, 58.

[116] Andrew C. DeVore, *Cloud Computing: Privacy Storm on the Horizon?*, 20 ALB. L.J. SCI. & TECH. 365, 369 (2010) (warning that cloud networks are "high value targets" on which hackers are beginning to focus).

[117] *See* Allan A. Friedman & Darrell M. West, *Privacy and Security in Cloud Computing*, ISSUES TECH. INNOVATION, Oct. 2010, at 6. For instance, non-U.S. companies may be avoiding data centers in the United States out of concern that the Patriot Act will provide the U.S. Gov-

Finally, the EAR's strict adherence to location-based export controls on nonphysical transfers is increasing the burden on companies striving to achieve regulatory compliance in a modern, global economy. The struggle to reconcile the extraterritorial aspects of the Internet with traditional national borders is hardly new or unique to export controls.[118] The EAR, though, are particularly susceptible to changes in business technology because of the subject matter regulated and the relationship between changes in technology and changes in business practices.[119] The prevalence of corporations spanning national borders and trends toward outsourcing are two examples of how communications technologies have changed the way businesses function on a fundamental, day-to-day basis; the EAR regulate the use of many of these communications technologies.[120] Cloud computing may be the best example of this phenomenon, providing an important opportunity to consider the future of dual-use export controls.

III. License Exception Cloud Computing

The best solution to the uncertainty regarding, and the possible overregulation of, cloud computing is to create a new license exception in the EAR: License Exception Cloud Computing ("License Exception CLC"). As was mentioned above, license exceptions allow exports, reexports, and deemed exports to occur without the required license so long as the exporter or reexporter meets certain conditions.[121] As a practical matter, the Secretary of Commerce could carry out this solution without any congressional action.[122] So long as it remains within the boundaries of the Export Administration Act, International Emergency Economic Powers Act, and a few other statutory

ernment with access to sensitive corporate information. *See* Paul Lanois, *Caught in the Clouds: The Web 2.0, Cloud Computing, and Privacy?*, 9 Nw. J. Tech. & Intell. Prop. 29, 45–46 (2010).

[118] *See generally* Gregory J. Wrenn, *Cyberspace is Real, National Borders are Fiction: The Protection of Expressive Rights Online Through Recognition of National Borders in Cyberspace*, 38 Stan. J. Int'l L. 97 (2002) (considering the question of legal jurisdiction over Internet activity).

[119] *See generally* Bowman, *supra* note 42, at 351–56.

[120] *See id.* at 359.

[121] *See supra* Part I.D.

[122] The Export Administration Act of 1979 provides that the Secretary of Commerce may impose conditions on the requirement of licenses that are "consistent with the provisions of [the Act]." Export Administration Act of 1979, Pub. L. No. 96-72, § 4(a), 93 Stat. 503, 505 (expired 1994). As an illustration of this authority, consider the new License Exception STA. This exception would remove the licensing requirements on a large number of items listed on the CCL without any change in congressional authority. Export Control Reform Initiative: Strategic Trade Authorization License Exception, 76 Fed. Reg. 35,276, 35,287 (June 16, 2011) (to be codified at 15 C.F.R. pt. 740).

limitations,[123] BIS has sufficient leeway to greatly decrease the burden on companies using cloud computing.

This Part introduces License Exception CLC, which would provide greater clarity and flexibility than the current regulatory approach. It presents and explains the language to be added to the EAR. It then provides the rationale behind the exception and examples of how this exception would apply to real export situations.

A. *Proposed Regulatory Language*

This Note proposes a new license exception for transmissions that occur when using cloud-based data storage. License Exception CLC would relieve cloud users of most licensing requirements that cannot be met because of uncertainty about the time and destination of cloud transmissions. It would require that cloud users take certain measures before uploading controlled technical data, and it would limit both the types of data and the cloud providers that could qualify for the exception.

The EAR should be amended to include the following exception:

740.21 License Exception Cloud Computing (CLC)[124]

(a) *Scope.* Controlled technology may be transmitted through a data storage network in lieu of a license that would otherwise be required pursuant to part 742 of the EAR. License Exception CLC does not authorize any new release of technology, but it does protect users from liability for unauthorized deemed exports to foreign nationals employed by the data storage provider. Any transmission to a foreign data storage provider or from the data storage provider to individuals located outside of the United States must be authorized in accordance with the other provisions of the EAR (e.g., through a license or license exception), or, alternatively, not require such authorization.

[123] *See, e.g.*, Export Control Modernization: Strategic Trade Authorization License Exception, 75 Fed. Reg. 76,653, 76,654 (proposed Dec. 9, 2010) (to be codified at 15 C.F.R. pt. 740) ("Items on the Commerce Control List that are subject to the short supply (SS), surreptitious listening (SL), missile technology (MT) or chemical weapons (CW) reasons for control would not be eligible for License Exception STA because of various requirements imposed by statutes, treaties or U.S. implementation of international commitments.").

[124] In subsequent citations, this proposed language will be identified as "Proposed License Exception CLC."

(b) *Requirements and Limitations*—(1) *Requirements for Using License Exception CLC.*

(i) At the commencement of the transmission from the party using License Exception CLC to the data storage network, the party must retain the following documentation for its records:

(A) The ECCNs of all items transmitted to the data storage provider; and

(B) A statement from the data storage provider

(1) affirming that the data storage provider will comply with all data security requirements issued by BIS;

(2) confirming that no network servers are or will be maintained in a destination identified in section 740.2(a)(6) of this part;[125] and

(3) affirming that all foreign nationals employed by the data storage provider will be required to sign binding nondisclosure agreements not to release any technology acquired through his or her employment with the data storage provider.

(ii) The documents required by paragraph (b)(1)(i) must be updated to reflect subsequent changes that make the information inaccurate.

(2) *Limitations on the Use of License Exception CLC.*

(i) License Exception CLC may not be used in lieu of any license requirement imposed by parts 744 or 746 of the EAR.

(ii) License Exception CLC does not authorize any transmissions of controlled technical data except those that occur between the party and a data storage network maintained by an eligible data storage provider or within such a data storage network.

(A) For purposes of this section, "data storage network" means a network of resources designed to provide virtualized storage, located within and/or outside of the United States, and accessible by the customer through the Internet.

(B) For purposes of this section, "data storage provider" means a commercial entity that maintains a data storage network and provides

[125] For the purposes of part 740, comprehensively embargoed nations are Cuba, Iran, and North Korea. 15 C.F.R. § 740.2(a)(6) (2011).

customers with data storage services accessible through the Internet.

(1) The same entity may not qualify as both a data storage provider and a customer;

(2) Foreign as well as U.S. entities can qualify as data storage providers, so long as release of the technology in question to this entity would not require a license.

(C) For purposes of this section, "eligible data storage provider" means a data storage provider that complies with all data security requirements issued by BIS.

(iii) License Exception CLC does not authorize any release of controlled technical data except inadvertent releases to foreign nationals employed by an eligible data storage provider, and only when said employee has entered into an agreement to not disclose any technology attained through said employee's employment by the data storage provider.

For purposes of this section, "inadvertent releases" means the release of any user-generated technical data required to screen content for valid law enforcement requests, troubleshooting individual accounts, or perform other duties for which the employee was employed.

(iv) License Exception CLC does not authorize transmissions to data storage providers that the party knows or has reason to know would provide foreign governments with access to private customer data.

B. Explanation

License Exception CLC would exempt users of cloud computing from obtaining a license before uploading certain controlled technology to a commercial cloud data storage network. As subsection 740.22(a) makes clear, the exception would not be available for releases of technology from the cloud to a third party that could not otherwise have access to the information.[126] However, it would allow both an original transmission from a user or provider to a foreign server or a subsequent transmission from one foreign server to another within the same data storage network. Finally, License Exception CLC would allow releases to foreign nationals employed by cloud

[126] *See supra* Proposed License Exception CLC § 740.22(a).

providers so long as those releases occur while the employee is performing her assigned duties.

The scope of License Exception CLC cannot be understood by just looking at its language. Certain restrictions found in 15 C.F.R. § 740.2 are applicable to all license exceptions. For instance, technology related to some items would be ineligible for export under License Exception CLC.[127] Also, no transmissions could be directed to Cuba, North Korea, or Iran.[128] Finally, License Exception CLC would not apply to any knowing or willful uses of cloud technology by prohibited end-users or for prohibited end-uses.[129]

License Exception CLC also limits which cloud providers qualify for receiving technology. First, cloud providers must ensure that all non-U.S. employees with access to user-generated content have agreed not to disclose any technology they come into contact with as part of their duties.[130] Second, and more importantly, License Exception CLC requires that the cloud provider meet data security requirements published by BIS in conjunction with License Exception CLC.[131] Though it is beyond the scope of this Note to propose specific security requirements, BIS would ideally rely on the security provisions of the Federal Risk and Authorization Management Program's

[127] These restrictions are based on statutory requirements or treaty terms beyond the regulatory authority of BIS. The restricted groups are (1) items and related software primarily useful for intercepting wire, oral, or electronic communications, 15 C.F.R. § 740.2(a)(3); (2) certain shotguns, law enforcement restraint devices, and items designed for execution, *id.* §§ 740.2(a)(4), .7; (3) most items controlled for Missile Technology reasons, *id.* § 740.2(a)(5); (4) technology related to traveling wave tube amplifiers and other space-qualified items, *id.* § 740.2(a)(7); and (5) technology related to explosives or detonator detection equipment, *id.* § 740.2(a)(8).

[128] *Id.* § 740.2(a)(6). Certain exceptions can apply to these countries individually or as a group. *See, e.g.*, *id.* § 746.2(a)(1) (allowing exports using specific license exceptions to Cuba). However, since the maintenance of cloud servers in any of these countries would contravene numerous other portions of the EAR and other sanctions legislation, such an expansion of License Exception CLC to these embargoed destinations does not seem necessary. *See* 31 C.F.R. § 515.201(b)(1) (2010) (prohibiting, with relation to Cuba, "[a]ll dealings in . . . any property . . . by any person subject to the jurisdiction of the United States"); *id.* §§ 560.206–.207 (prohibiting transactions with and investment in Iran).

[129] General Prohibition Five prohibits such exports. 15 C.F.R. § 736.2(b)(5); *see also id.* § 740.2(a)(2) (restricting the application of license exceptions to exports subject to a general prohibition).

[130] *See supra* Proposed License Exception CLC § 740.22(b)(2)(iii). This addresses the problem of deemed exports to employees of cloud providers. *See supra* notes 98–99 and accompanying text. The use of nondisclosure agreements to address possible deemed exports within a company is similar to that proposed as part of License Exception Intra-Company Transfer, which was proposed in 2008 but never finalized. *See* Establishment of License Exception Intra-Company Transfer (ICT), 73 Fed. Reg. 57,554, 57,560 (proposed Oct. 3, 2008) (to be codified at 15 C.F.R. pt. 740).

[131] *See supra* Proposed License Exception CLC § 740.22(b)(1)(i)(B)(1).

Cloud Computing Security Requirements Baseline ("FedRAMP Guidelines").[132]

License Exception CLC would regulate other aspects of the relationship between cloud user and cloud provider. If a company set up its own private cloud using servers located outside of the United States, License Exception CLC would not allow any exports of controlled technology.[133] In these situations, the cloud user/provider would have control over where its information is stored and should be better positioned to make certain that unauthorized transmissions do not occur. Additionally, License Exception CLC could only be used when the cloud provider is an entity that can receive the information without causing a deemed export violation.[134] Finally, the user could not knowingly or recklessly transmit data to a provider that might make this controlled information available to foreign governments.[135]

After determining that none of License Exception CLC's limitations apply to a desired transaction, the cloud user would need only internal monitoring and documentation from the cloud provider. First, the user would be required to consider all the technical data it wished to store on the cloud and identify the ECCNs of all items transmitted to the provider.[136] The ECCNs of those items would have to be recorded and periodically updated.[137] Users of the exception would also be required to collect statements from their cloud provider on compliance with the BIS security guidelines and foreign national

[132] *See generally* FED. CHIEF INFO. OFFICER COUNCIL, PROPOSED SECURITY ASSESSMENT & AUTHORIZATION FOR U.S. GOVERNMENT CLOUD COMPUTING 3–34 tbl.1 (2010) (listing the FedRAMP Guidelines). The FedRAMP Guidelines were designed to ensure adequate protection of government data on the cloud, and thus should include security that is more than adequate for dual-use technology. *See id.* at i. Because many cloud providers are likely to meet FedRAMP standards in order to be eligible for government cloud computing contracts, using these standards would ensure that enough providers are eligible to store dual-use technical data under License Exception CLC. *See infra* Part III.C.1.

[133] *See supra* Proposed License Exception CLC § 740.22(b)(2)(ii)(B)(1).

[134] *See supra* Proposed License Exception CLC § 740.22(b)(2)(ii)(B)(2). This would create a group of foreign data storage providers that could not receive technology, because of the deemed export rule, that License Exception CLC otherwise would allow to be transmitted within a cloud network. *See generally supra* Part I.C. However, a license for this original transmission to the cloud provider would not face the problems normally associated with cloud computing because the nationality of the entity would be easily discernible. *See generally supra* Part I.D.

[135] *See supra* Proposed License Exception CLC § 740.22(b)(2)(iv). For instance, if there have been reports that a cloud provider has surrendered cloud user data to the Chinese government, License Exception CLC could not apply to any transmissions to this cloud provider.

[136] *See supra* Proposed License Exception CLC § 740.22(b)(1)(i)(A).

[137] *See supra* Proposed License Exception CLC § 740.22(b)(1)(ii).

nondisclosure agreements.[138] Finally, data storage providers would be obligated to confirm that no network servers would be maintained in Iran, North Korea, or Cuba.[139] Under the EAR's general recordkeeping policy, cloud users would retain the documents until five years after all EAR-controlled technology is removed from the cloud.[140]

C. Rationale of License Exception CLC

These provisions reduce regulatory barriers to the use of cloud computing without undermining the EAR's national security goals. Of course, given the present confusion about how export controls apply to cloud computing, any regulation would allow both cloud service providers and potential cloud users to weigh economic benefits against regulatory costs.[141] However, this Section highlights the ways in which License Exception CLC reflects a more sophisticated understanding of the cloud computing problem by allocating requirements according to the information available to each party and by recalibrating the EAR to address the real security threats of cloud computing.

1. Placing the Regulatory Burden on Those with Access to Information

One of the most important aspects of the proposed exception's design is its allocation of the regulatory burden between cloud computing users and providers. By clarifying BIS's regulatory stance, the exception would increase awareness among cloud computing providers of their services' export control implications. Though the requirements are not directly placed on them, cloud providers would have economic incentives to ensure that they provided their services in a manner that would not cause their customers to run afoul of applicable regulations. Therefore, providers that maintain servers outside the United States would discuss the export control requirements with prospective customers. This would address the initial problem of ensuring that cloud users, who may not know that they could export

[138] *See supra* Proposed License Exception CLC § 740.22(b)(1)(i)(B)(1).

[139] *See supra* Proposed License Exception CLC § 740.22(b)(1)(i)(B)(2). Some cloud providers already provide such assurances. *See VMware Export Control Policy*, VMWARE, http://www.vmware.com/help/export-control.html (last visited Dec. 26, 2011) ("VMware prohibits any export or re-export of VMware products, services, or technical data to any destinations subject to U.S. embargoes or trade sanctions.").

[140] *See* 15 C.F.R. § 762.6 (2011).

[141] *See, e.g.*, Curran, *supra* note 108 ("Ultimately, cloud providers and users would benefit from greater clarity regarding how to comply with U.S. trade control laws under various cloud computing scenarios.").

their technology by uploading it to the cloud, would become aware of the EAR's applicability to cloud use.[142]

Moreover, only cloud users would be able to assess the EAR's application to their use of the cloud. Given the large amounts of data that cloud providers receive and the privacy concerns that users have, only individual users can be expected to know the export controls on specific technologies placed on the cloud. By requiring cloud users to take inventory of which technologies are on the CCL, License Exception CLC would ensure that these companies would consider what information is controlled and whether any items fell outside of the scope of the exception.

Finally, the requirements placed on cloud providers would allow sufficient protection for business secrets and ensure basic data security. The license exception would only require certification that the providers were not placing servers in embargoed destinations,[143] rather than the exact locations of these foreign servers, because the latter information is irrelevant from an export control standpoint.[144] Cloud providers would also have better access to information about their own network security and employees. All of these provisions would create a means of oversight over cloud providers to ensure sufficient precautions are taken.[145]

2. *Recalibrating the EAR to Address National Security Threats*

License Exception CLC is also designed to make the EAR more responsive to the unique threats that cloud computing could pose. By not requiring the cloud user to provide any information about the destination of the export, this exception would circumvent the primary problem facing customers who wish to use cloud computing in an EAR-compliant manner.[146] This would not undermine U.S. national security goals because the location of a server is a poor indicator of

[142] In conjunction with this rulemaking, BIS should incorporate the compliance risks of cloud computing into the agency's numerous exporter education efforts. *See, e.g.*, *Seminars and Training*, U.S. BUREAU INDUS. & SEC., http://www.bis.doc.gov/seminarsandtraining/index.htm (last visited Dec. 26, 2011).

[143] *See supra* Proposed License Exception CLC § 740.22(b)(i)(B)(2).

[144] *See supra* notes 112–13 and accompanying text.

[145] Although the 2009 and 2011 advisory opinions greatly limit the potential liability of cloud providers, these actors play an important role in protecting controlled data from governmental and nongovernmental actors. *See supra* Part II.B. If providers are engaged in risky behavior and make false statements about data security to BIS, the U.S. Customs Service, or an official of any U.S. agency, these requirements could allow BIS to bring charges of "misrepresentation or concealment of fact" under the EAR. 15 C.F.R. § 764.2(g)(1).

[146] *See supra* text accompanying note 110.

how susceptible information on that server is to diversion.[147] The exception to this broad discounting of location is the fact that there could be no cloud exports to Iran, North Korea, or Cuba.[148] This limitation does not reflect concerns that information on a server in Cuba is more vulnerable than in other countries; rather, it is a reflection of the numerous other controls and sanctions imposed on some countries.[149]

Though it deemphasizes location, License Exception CLC's structure would maintain other important aspects of the EAR. For instance, the exception would not apply to any knowing or willful uses of cloud technology involving prohibited end-uses or end-users.[150] Also, the exception would not change how access to the cloud from outside the United States would be treated.[151] These transmissions raise the same export control problems as any technology export, and thus should not be treated differently solely because of the technology used.[152] Additionally, the technologies that have traditionally elicited the most concern (e.g., missile technology, space-qualified items, etc.) would remain ineligible for any license exceptions and could not be placed on the cloud.[153]

Finally, License Exception CLC would better address the goals of the EAR in the context of cloud computing. BIS's security guidelines, which all cloud providers would have to meet in order to enable their customers to use License Exception CLC, would decrease the possibility of unauthorized access of controlled information on the cloud by governmental or nongovernmental actors. Location-based controls cannot address the threat of network vulnerabilities because such intrusions could occur over the Internet from any location.[154] And although foreign governments could try to use their regulatory or judicial powers to access the cloud,[155] License Exception CLC does not allow users to transmit data if they know or have reason to know this outcome will occur.[156]

[147] *See supra* notes 112–13 and accompanying text.

[148] *See supra* Proposed License Exception CLC § 740.22(b)(i)(B)(2).

[149] *See supra* note 128.

[150] *See supra* Proposed License Exception CLC § 740.22(b)(2)(i). This limitation extends to cloud computing providers. *See* 2009 Advisory Opinion, *supra* note 15, at 2.

[151] *See supra* Proposed License Exception CLC § 740.22(b)(2)(ii).

[152] *See supra* notes 39–41 and accompanying text.

[153] *See supra* note 127 and accompanying text.

[154] *See supra* text accompanying notes 112–13.

[155] *See supra* note 117 and accompanying text.

[156] *See supra* Proposed License Exception CLC § 740.22(b)(2)(iv). Because users already have a strong incentive to avoid such situations, paragraph (b)(2)(iv) need not be stricter.

D. Examples of Application of License Exception CLC

In all cases involving License Exception CLC, data storage providers would take certain preliminary steps to ensure compliance. If providers with servers outside the United States wished to attract customers who have U.S.-regulated dual-use technology—likely a sizeable portion of the possible market—they would implement the BIS security guidelines, enter into binding nondisclosure agreements with foreign national employees, and avoid installing servers in Iran, North Korea, and Cuba.

This Section considers three situations from the perspective of a potential cloud user with items subject to the EAR. The first portrays a successful application of License Exception CLC and compares this with the outcome under the current regime. The second illustrates a situation in which a company wishes to upload data but the exception cannot be applied. Finally, the third example involves an unacceptable use of the cloud to transmit information to another party.

1. Successful Application of License Exception CLC

Consider a company that designs and manufactures chemicals. Hoping to provide for more communication and collaboration between its multiple U.S. offices during the design process, the company considers transferring its data to a cloud data storage service. While negotiating with a cloud provider that maintains servers outside of the United States, the company becomes aware of the possible regulatory concerns related to export controls.

After considering the data to be transferred to the cloud, the company's attorney finds that most of the company's information is not for items on the CCL, is not subject to any license requirements, and can be uploaded without further action. However, she also recognizes that some specific chemicals are precursors for toxic chemical agents, and are classified under ECCN 1C350.[157] Therefore, the information about their design and production is controlled under ECCN 1E350 for Chemical and Biological Weapons and Anti-Terrorism reasons.[158] According to the EAR's Commerce Country Chart, a license would be required for the transmission of this information to almost any non-European nation.[159]

[157] 15 C.F.R. pt. 774, supp. 1 (2011).

[158] *Id.*

[159] *Id.* pt. 740, supp. 1. If the user knew that no transmission would occur outside of the United States or Europe, no violation could possibly occur and License Exception CLC would

Under the EAR as they exist today, this license (or another license exception) would not be available. Because of the cloud provider's security and competition concerns, the provider might be unwilling to share information about the location of its data centers.[160] Even if the provider did share this information, the cloud user would not know to which destination the information would be transmitted,[161] and neither license applications nor existing license exceptions would be available.[162] This manufacturer could not upload the information to the cloud without risking a violation of the EAR.

With License Exception CLC, however, the company could store this data on the cloud. As information is transferred from the company to its new virtual machine on the cloud, the user's attorney would document the ECCNs of the controlled items.[163] This list would not be submitted to BIS unless there is a problem, and no approval by the Department of Commerce would be necessary. Rather, the list of ECCNs—along with the provider's certifications about (1) its compliance with the BIS security guidelines, (2) the policy requiring nondisclosure agreements with foreign national employees that have access to user-generated content, and (3) a lack of data centers in embargoed destinations[164]—would be kept until five years after the company removed all of the export-controlled technology from the cloud.[165] No matter where the servers were located or how often the data were transferred, there would be no violation of the EAR. Nor would there be a violation if a foreign national employed by the cloud provider inadvertently accessed this data while, say, troubleshooting the company's account.

2. *Transmitting Items to the Cloud that Are Excluded from the Exception*

Meanwhile, consider a second company that designs chemical manufacturing equipment. This company also wishes to use cloud storage for the same efficiency and collaboration reasons listed above. It also becomes aware of the export control issues related to cloud computing while negotiating with cloud providers.

not be necessary. However, fulfilling the exception's requirements would ensure that future expansions of the cloud network would not lead to violations.

[160] *See* Fleischer, *supra* note 84.

[161] *See id.*

[162] *See supra* Part I.D.

[163] *See supra* Proposed License Exception CLC § 740.22(b)(1)(i)(A).

[164] *See supra* Proposed License Exception CLC § 740.22(b)(1)(i)(B).

[165] *See* 15 C.F.R. § 762.6 (2011).

The company's attorney looks into the EAR's restrictions on the various chemical manufacturing equipment that the firm produces. She notices that some of the batch mixers meet the specifications listed in the CCL under ECCN 1B117.[166] She also notes that technology for these mixers is controlled under ECCN 1E001 for Missile Technology and Anti-Terrorism reasons.[167] License exceptions can be used to export a few Missile Technology items, but ECCN 1E001 is not one of them.[168] Therefore, License Exception CLC would not be available for this proposed data transfer. Even if the company gathers all the necessary records before uploading this data to the cloud server, transmissions to a server in a country where a license is required would violate the EAR.

3. *Accessing the Cloud Outside of the United States*

Finally, recall the chemical company described in the first example. Instead of only allowing its domestic offices to access the data on the cloud, suppose that this company now wants to extend access to a subsidiary in Brazil. The subsidiary has both American and Brazilian employees. If a Brazilian employee were able to access the data, this would constitute a deemed export requiring a deemed export license from BIS.[169] However, even if only American employees were allowed to access the cloud, transferring this data from the cloud to a local computer in Brazil to edit it would be a transmission of controlled technology and could require a license.[170]

Although License Exception CLC would still protect the company from any violations related to the transmission of the data to the cloud provider's foreign server (including a server in Brazil), the exception would not protect the company either from the export or deemed export violations noted above. When the data storage provider no longer has control over the data, any transmissions would be treated as an export where traditional EAR rules applied.[171] Simi-

[166] ECCN 1B117 includes batch mixers that can mix between 0 and 13.326 kilopascals, and have temperature control capability, a total capacity at or above 110 liters, and at least one kneading shaft mounted off-center. *Id.* pt. 774, supp. 1.

[167] ECCN 1E001 includes technology for the development or production of all items controlled under ECCNs beginning with "1B"—i.e., items that relate to test, inspection, or production equipment. *Id.*

[168] *See supra* note 127 and accompanying text.

[169] *See supra* text accompanying notes 43–44, 46. A license is required because items controlled for Chemical and Biological Weapons reasons require a license for export to Brazil according to the Commerce Country Chart. 15 C.F.R. pt. 738, supp. 1.

[170] *See supra* notes 39–40 and accompanying text.

[171] *See supra* Part I.D. The 2009 advisory opinion suggests that the cloud provider would

larly, if a non-U.S. national in the United States has access to the cloud as an employee of the user, the normal deemed export requirements would apply.[172]

IV. Counterarguments

This Section considers several counterarguments that could be leveled against the establishment of License Exception CLC. Because the U.S. export control regime faces simultaneous criticism from different interest groups for being both too lax and too rigid,[173] this Section considers the problem from the perspective of the national security community and the business community.

A. License Exception CLC Would Excessively Decrease Export Requirements

The first argument against License Exception CLC is that decreasing export controls on the cloud would expose the United States to greater security threats. Export controls are designed to keep U.S. technologies out of the hands of individual or state actors who might use them to undermine U.S. foreign policy goals.[174] However, License Exception CLC would curtail BIS's licensing oversight of an unknown number of transmissions of controlled technology. This could lead to numerous exports, reexports, or deemed exports to cloud employees. Therefore, according to this view, liberalization through License Exception CLC should not proceed.

The flaw in this argument is its focus on the *items* being exported rather than the *means* of export. Even if a transmission of controlled information to a foreign server did occur, this transfer would not pose

not be liable in this instance. *See* 2009 Advisory Opinion, *supra* note 15, at 3. Noting that the provider does not receive a "benefit" from the transaction, the opinion states that the provider could not be the "exporter" and thus could not be liable. *See id.*

[172] *See supra* Proposed License Exception CLC § 740.22(b)(2)(ii). Other license exceptions or the procurement of export or deemed export licenses could allow the company to act in this manner without incurring liability, but License Exception CLC would not.

[173] *Compare, e.g., The Export Administration Act: A Review of Outstanding Policy Considerations: Hearing Before the Subcomm. on Terrorism, Nonproliferation and Trade of the H. Comm. on Foreign Affairs*, 111th Cong. 22 (2009) (statement of Arthur Shulman, General Counsel, Wisconsin Project on Nuclear Arms Control) ("The focus of export control reforms should be on ensuring that the system protects U.S. national security in the 21st century—not on removing the remaining speed bumps on the export superhighway."), *with Earthbound*, Economist, Aug. 23, 2008, at 66, 66 (reporting that critics of export controls believe that the United States has "erred on the side of stifling").

[174] *See* 15 C.F.R. § 730.6 (noting that a purpose of export controls is to "restrict access to dual-use items by countries or persons that might apply such items to uses inimical to U.S. interests").

the same risks as other nonphysical exports.[175] BIS has suggested that exports in which the exporter and the recipient are the same entity might not require the same level of control, though the agency has not codified this concept in the EAR.[176] Moreover, this solution would be consistent with the EAR's increasing focus on end-use and end-user concerns rather than the item in question.[177] All of these factors lead to the conclusion that reduced licensing requirements for cloud computing transmissions would be consistent with the form and underlying rationale of the EAR.

B. License Exception CLC is Too Risky Due to Data Security Concerns

A second argument is that this exception does not adequately address concerns about the security of data stored on the cloud. The unique data security challenges that cloud computing poses are undeniable. Single networks with large collections of data create attractive targets for hackers.[178] If state or nonstate actors gained unauthorized access to a cloud network and misappropriated dual-use technology, this would have adverse effects on U.S. national security and foreign policy.[179]

Though policymakers must not lose sight of these concerns, data security does not make License Exception CLC untenable. It is worth noting that the EAR do not require absolute security in other technology export contexts. For instance, BIS does not consider encryption source code made available on the Internet to be exported if "the person making the software available takes precautions adequate to prevent unauthorized transfer."[180] Also, License Exception Temporary Imports, Exports and Reexports allows U.S. persons or their employees to temporarily export technology to foreign countries without a

[175] *See supra* notes 112–13 and accompanying text.

[176] Proposed License Exception Intra-Company Transfer attempted to deal with similar concerns. *See* Establishment of License Exception Intra-Company Transfer (ICT), 73 Fed. Reg. 57,554 (proposed Oct. 3, 2008) (to be codified at 15 C.F.R. pts. 740, 772). License Exception Intra-Company Transfer would have decreased restraints on transfers of controlled items within a company structure based on the decreased likelihood that the items would be released to the host country. *See id.* A key element of this exception was the approval of a "control plan" to ensure items would not leave the company. *Id.* at 57,560. In the context of cloud computing, there is even less of a likelihood that controlled information might "leak out" because of the limited access to cloud information.

[177] *See* Bowman, *supra* note 42, at 344.

[178] *See* DeVore, *supra* note 116, at 468–69.

[179] *See supra* note 115 and accompanying text.

[180] 15 C.F.R. § 734.2(b)(9)(ii) (2011).

license subject to enumerated restrictions.[181] In these situations, the temporary exporter must provide certain levels of data security (e.g., password protection or firewalls) to ensure against unauthorized access.[182]

Critics might distinguish the laxer standards for temporary exports from the data storage context because, in the latter situation, more data is amassed on a foreign server for a longer period of time. These risks may be greater, but so would the security measures protecting information on cloud servers. License Exception CLC would require cloud providers to implement basic security measures set out by BIS before becoming eligible to receive controlled data.[183] In addition, although many companies lack the necessary funding and expertise to ensure that their networks have the highest level of security available, cloud providers do not.[184] The same level of efficiency that firms achieve by allowing cloud providers to specialize in handling IT maintenance is also achieved in data security.[185] More directly, cloud users are not likely to use a service that they feel leaves their data (export-controlled or otherwise) vulnerable. Cloud providers thus have an existential interest in providing the best security to current and prospective clients, and market forces will lead to better data protection.[186]

Finally, this counterargument does not cut against foreign transmissions to untrustworthy nations alone; rather, it would prohibit *all* uses of cloud computing for export-controlled technologies. This position would even prohibit the use of cloud servers located in the United States because users of these services still rely on the provider for data protection.[187] If such providers were deemed unfit to handle

[181] *Id.* § 740.9(a)(1).

[182] *Id.* § 740.9(a)(3)(iv)(B).

[183] *See supra* Proposed License Exception CLC § 740.22(b)(1)(i)(B).

[184] *See* Hugos & Hulitzky, *supra* note 5, at 91–92 (arguing that cloud security should be favorably compared to existing security of computer networks, which is characterized by a lack of expertise and funding in many IT departments); DeVore, *supra* note 116, at 368 ("Most small and medium-sized companies just don't have the resources to provide the security that they should have in place to protect their electronically stored information.").

[185] *See* Hugos & Hulitzky, *supra* note 5, at 91–92. Google made a similar point after suffering an attack on its network, claiming that, "[w]hile any company can be subject to such an attack, those who use our cloud services benefit from our data security capabilities." Dave Girouard, *Keeping Your Data Safe*, Official Google Enterprise Blog (Jan. 12, 2010), http://googleenterprise.blogspot.com/2010/01/keeping-your-data-safe.html.

[186] *See* Hugos & Hulitzky, *supra* note 5, at 91–92 (noting that security is "mission-critical to customer retention and profits" for cloud providers, making them "far more inclined to invest in more than adequate security").

[187] *See supra* note 114 and accompanying text.

any export-controlled technical data on a foreign server, there would be no way to distinguish domestic uses of the cloud either. Unless the United States is willing to accept this extremely restrictive outcome, some line should be drawn according to the real threats involved. These concerns would be reason for BIS to proceed cautiously with License Exception CLC, but not to disqualify the exception altogether.

C. *Restrictions and Compliance Costs Would Limit this Exception's Effect*

From the opposite viewpoint, License Exception CLC could face criticism for being too limited and costly to relieve pressure on the burgeoning cloud computing industry. The identification, classification, and recording of controlled technologies placed on the cloud would require expenditures that could dissuade possible users. Moreover, removing some items from the scope of the exception, such as those controlled for Missile Technology reasons, would exclude a portion of the technologies that users might want to upload to the cloud. All of these factors would decrease the number of companies willing or able to use the exception, purportedly resulting in minimal changes to the status quo.

Compliance costs for cloud users would surely exist, but License Exception CLC would not increase these costs prohibitively. It seems fair to assume that most of the companies seeking to use cloud systems to store controlled data already have export-compliance programs in place, which would generally include classification of technology. Thus, the additional costs of keeping records would be minimal because most of the work would already have been done. More directly, cloud users are currently advised to classify their controlled data and keep it off of the cloud.[188] License Exception CLC can hardly be criticized for increasing the cost of compliance when currently the same practices are required.

Some companies may be unable to afford these compliance costs or would wish to use the license exception for technologies outside of the exception's scope, but complaints on their behalf should not derail this Note's proposed solution. License Exception CLC is intended to facilitate exports of technology to the cloud, but it could not eliminate all restrictions on these exports. Companies that could not meet these requirements would not be able to use the cloud in a responsible man-

[188] *See Cloud Computing Provides Unique Export Control Challenges*, *supra* note 17, at 13.

ner for controlled items. They would not know what controlled technology they have placed on the cloud and thus could be more careless with respect to who they allow to access it. With regard to the scope of the exception, the License Exception CLC cannot be expanded any further without contravening applicable statutes or treaties.[189] The fact that some companies could not use this exception should not bar its adoption.

D. *Fundamental Changes to the EAR's View of Nonphysical Exports Should Be Made*

Those espousing the argument above might go one step further, calling for cloud computing transmissions to no longer be viewed as exports regulated under the EAR. As this Note argues, the threats posed by cloud computing transmissions are drastically different from those posed by traditional exports or even other nonphysical exports because there is no change of ownership or access to the information.[190] Given this fact, one might argue that these transmissions should not be considered exports at all, and thus should not require a license.

Though tempting in its simplicity, this approach is ill advised. The fact that some of the ways cloud computing would be used do not pose export control threats does not mean that all regulatory oversight should be removed.[191] There is still the likely possibility that actors would use cloud computing to transmit data between individuals, which would remain an export subject to a license requirement.[192] Removing cloud computing from the scope of the EAR could make regulation of these transactions more difficult to enforce and lead to greater confusion in the regulated community.[193] Put another way, the debate surrounding export controls on cloud computing is too intertwined with the larger concern of nonphysical transactions to be effectively addressed by a narrow, but sweeping, jurisdictional change.

That is not to say that more drastic changes are unnecessary. This Note does not try to hide the fact that, given Congress's reticence to renew or update the Export Administration Act, the appeal of Li-

[189] *See supra* note 127.

[190] *See supra* notes 112–17 and accompanying text.

[191] *See* VILLASENOR, *supra* note 19, at 9 ("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.").

[192] *See supra* Part III.D.3.

[193] *See* VILLASENOR, *supra* note 19, at 9.

cense Exception CLC is directly related to its practicability.[194] Since the passage of the Act in 1979, corporations have dispersed around the world while growing more interconnected. There are growing concerns about the effectiveness, enforceability, and economic impact of the Act's approach to nonphysical exports.[195] These concerns are not addressed by President Obama's Export Control Reform Initiative.[196] License Exception CLC is best viewed as a stopgap to allow the technology and business practices surrounding cloud computing to develop while Congress has time to consider and pass new legislation with a more modern approach to nonphysical exports.

Conclusion

The use of cloud computing technology falls within the U.S. export control regime but does not pose the same national security concerns as other physical and nonphysical exports. To relieve regulatory uncertainty and allow for the development of this important technology, BIS should create a license exception for transmissions to cloud servers outside of the United States. This exception would allow cloud users to upload information without knowing if or when an international transmission would occur and place minimal requirements on both cloud users and cloud providers. In so doing, this exception would protect the United States' national security goals and allow businesses to take advantage of this important new technology.

[194] *See supra* note 122 and accompanying text.

[195] *See generally* Bowman, *supra* note 42.

[196] President Obama has proposed and is carrying out several changes to the U.S. export control regime, including consolidating the U.S. Munitions List and the CCL into one positive list of controlled items, and creating one agency to regulate export controls. Press Release, The White House, Office of the Press Sec'y, Fact Sheet on the President's Export Control Reform Initiative (Apr. 20, 2010), *available at* http://www.pmddtc.state.gov/documents/WhiteHouseFact Sheet.pdf.