United States Export Controls on Internet Software Transactions

John F. McKenzie
Partner, Baker & McKenzie LLP

August 2010
# Table of Contents

1. Introduction ................................................................................................................ 1
2. The Concept of an "Export" for Export Control Purposes ........................................ 2
3. Export Control Status of Application Software Products ........................................ 3
5. Conclusion ................................................................................................................ 12
1. Introduction

The United States maintains a comprehensive program of controls on the export and reexport of commodities, software and technology under a series of regulatory programs. Defense items, as specified on the United States Munitions List or as otherwise specially designed, modified, customized or adapted for military use, are subject to the munitions export control program set forth in the International Traffic in Arms Regulations, 22 C.F.R. Parts 120-130 (the "ITAR"), which are issued under authority of the Arms Export Control Act, 22 U.S.C. § 2778, and are administered by the State Department's Directorate of Defense Trade Controls.

Commercial (or "dual use") commodities, software and technology are subject to export controls under the Export Administration Regulations, 15 C.F.R. Parts 730-774 (the "EAR")1. Those commercial export controls, which are administered by the Commerce Department's Bureau of Industry and Security, are directly applicable to most software export transactions, and are, therefore, the focus of this paper.

The export controls embodied in the EAR are implemented by a licensing procedure, under which the prior authorization from the Bureau of Industry and Security, in the form of an export license, may be required for certain export or reexport transactions, depending on:

(i) the export classification and export control status of the commodities, software or technology involved in the transaction2;

(ii) the destination or destinations to which those commodities, software or technology will be exported or reexported3;

(iii) the identity of the end-user to which the commodities, software or technology will be supplied4; and

---


2 Commodities, software and technology that are subject to export controls under the EAR are listed on the Commerce Control List, which is published as Supplement No. 1 to Part 774 of the EAR. Those controlled items are organized by export classification control number or "ECCN". Each ECCN entry on the Commerce Control List provides a detailed description by technical specifications or performance parameters of the items subject to control, the reasons why that item is controlled (e.g., national security, nuclear non-proliferation, chemical and biological weapons proliferation, anti-terrorism, etc.), and the "export license exceptions" that may be available for the export or reexport of the items to some foreign countries.

3 Controlled countries, as defined in section 772.1 of the EAR, include Armenia, Azerbaijan, Belarus, Cambodia, Cuba, China, Georgia, Iraq, Kazakhstan, Kyrgyzstan, Laos, Macau, Moldova, Mongolia, North Korea, Russia, Tajikistan, Turkmenistan, Ukraine, Uzbekistan and Vietnam. Many items that may be exported without restriction or under an export license exception to other countries require a specific export license from the Bureau of Industry and Security for export to any of those controlled countries. Moreover, there are comprehensive embargoes on exports or reexports of all or substantially all items subject to the EAR to Cuba, Iran, North Korea, Sudan and Syria.

4 The United States Government maintains a series of lists of prohibited and restricted persons and firms (e.g., the Commerce Department's Denied Parties List; the Commerce Department's Entity List; the Treasury Department's OFAC list of specially designated nationals and blocked persons). Those lists of prohibited and restricted parties may be found on the Bureau of Industry and Security's website, at www.bis.doc.gov/complianceandenforcement/liststosearch.htm. The export or reexport of any item subject to the

Baker & McKenzie United States Export Controls on Internet Software Transactions 1
In any transaction involving the export or reexport of items subject to the EAR, it is the "exporter" that is legally responsible for determining, based on the foregoing factors, whether the transaction: (i) is authorized without an export license (i.e., the items are eligible for export under "NLR" or no license required); (ii) meets the conditions, requirements and restrictions of an "export license exception" as specified in Part 740 of the EAR; or (iii) requires an export license from the Bureau of Industry and Security. For this purpose, the term "exporter" is defined in section 772.1 of the EAR as: "The person in the United States who has the authority of a principal party in interest to determine and control the sending of items out of the United States.

As discussed in this paper, transactions that involve the export of software by means of electronic transmission or download over the internet present significant export compliance challenges, especially where the exporter: (i) is not the developer of the software; and (ii) has little or no information about the customer. Under such circumstances, the exporter may be unable to make an independent determination as to the ECCN export classification of the software product in question, and may have no information as to the identity, location or intended user of the software or the customer.

There is a third regulatory program that may restrict internet transactions involving United States origin software. Specifically, the various Economic Sanctions Regulations, 31 C.F.R. Parts 500 et seg., issued and administered by the Treasury Department's Office of Foreign Assets Control ("OFAC") under authority of the International Emergency Economic Powers Act, 50 U.S.C. § 1701 et seq., generally prohibit the export or reexport of United States origin goods, technology (including software) and services to (i) countries that are subject to comprehensive United States Government embargoes (i.e., Cuba, Iran and Sudan); (ii) entities, wherever located, that are owned or controlled by, or affiliated with, the governments of those embargoed countries; (iii) the governments of certain terrorist-supporting countries (e.g., Syria); (iv) international terrorists and foreign terrorist organizations; and (v) persons and firms listed on the OFAC list of specially designated nationals and blocked persons. As discussed in this paper, the potential application of those OFAC Economic Sanctions Regulations implies that entities making software or services available over the internet must screen the parties to proposed transactions, in order to assure that the software or services will not be received in an embargoed country, or by a person or entity on the OFAC list of specially designated nationals and blocked parties.

2. The Concept of an "Export" for Export Control Purposes

In the early days of the software industry, substantially all software transactions involved the physical shipment and delivery of a tangible embodiment of the software product (i.e., software encoded on some form of carrier media, such as a magnetic tape, disk, CD-ROM or DVD). With the advent of the

---

(iv) the intended end-use of the commodities, software or technology

---

5 Items that may otherwise be freely exported to almost any foreign country without restriction or prior authorization, require export licenses from the Bureau of Industry and Security for export to certain countries if, at the time of export, the exporter knows (or should know) that the items may be used in activities directly or indirectly related to the proliferation of nuclear, chemical or biological weapons or missiles.
internet, and the tremendous growth in e-Commerce transactions involving software products, a very significant and growing percentage of all commercial software "fulfillments" or deliveries involve electronic transmissions or downloads of the software code, where there is no shipment of any tangible item from the supplier to the customer. In many such electronic software transactions, especially those involving consumer or mass market software products, the software supplier is likely to have little or no direct interaction with, or knowledge of, its customer, other than a credit card number and an e-mail address.

Unlike export control regimes in a number of other countries, the EAR makes no distinction, for United States export control purposes, between the physical shipment of tangible items from the United States to a foreign country, and the electronic transmission of software or technology from the United States to a person or entity located abroad. For export control purposes, any such physical shipment or electronic transmission is an "export", which must be effected in conformance with the requirements and restrictions embodied in the EAR. Thus, section 734.2(b)(1) of the EAR defines the term "export" to include any "actual shipment or transmission of items subject to the EAR out of the United States".

As discussed in more detail in Section 3 of this paper, infra, a key factor in determining whether a particular software product is a controlled item under the EAR is the presence of any data encryption function or features in that software product. Section 734.2(b)(9) of the EAR sets forth a special, and expansive, definition of the concept of an "export" with respect to such encryption software, in source code or object code form. Under that section 734.2(b)(9), an "export" of encryption source code and object code software occurs when:

(i) there is an actual shipment, transfer or transmission of that encryption software out of the United States;

(ii) the software is downloaded to locations outside of the United States (including electronic bulletin boards, Internet file transfer protocol (FTP) sites, and World Wide Web sites); and

(iii) the software is "made available" for transfer outside of the United States, by means of posting to communications facilities that are accessible to persons outside of the United States (including electronic bulletin boards, FTP sites and World Wide Web sites), unless steps are taken to prevent unauthorized transfer of that encryption software.

These provisions of the EAR, defining the concept of an "export" to include the electronic transmission of software to locations outside of the United States, and the making of software (at least encryption software) available for download by persons located outside of the United States, imply that a software supplier that proposes to fill orders for its products electronically, or to make software products available for download by its customers from the supplier's website or on-line store, has the same export compliance responsibilities under the EAR as does any entity that makes physical export shipments of tangible items (commodities, software or technology) to customers located outside of the United States.

3. Export Control Status of Application Software Products

As noted in Section 1 of this paper, supra, one of the fundamental elements in assuring that software export transactions, including internet transactions, are handled in compliance with the export control requirements of the EAR is the determination of the correct export classification (ECCN) and control status of the software product to be exported. There are essentially two rubrics under which a particular
application software product may be classified as a controlled item for export control purposes under the EAR, as follows:

a. A number of controlled ECCN categories on the Commerce Control List cover software that is specially designed for the development, production or use of controlled commodities. Thus, for example, ECCN 3D003 imposes export controls on certain CAD software for the design of semiconductor circuits. Correspondingly, ECCN 5D001 imposes export controls on software that is required for the use of controlled telecommunications equipment.

b. Subject to certain limited exceptions, application software products are classified under ECCN 5D002, and are subject to strict export controls, if those products contain or support data encryption functionality or features. Exceptions exist for software products that: (i) use encryption technology solely for user authentication, password protection or other forms of access control; or (ii) utilize or support only very weak encryption functionality (i.e., a symmetric encryption algorithm with a key length not exceeding 56 bits; an asymmetric encryption algorithm with a key length not exceeding 512 bits). If a software application with encryption functionality does not, however, fall within the scope of one of those exceptions, it will be subject to the encryption (El) export controls, and prior authorization from the Bureau of Industry and Security will be required in order to export or reexport that software application6.

The Cryptography Note to the Commerce Control List indicates that certain "mass market" encryption software products are not subject to the strict encryption export control regime. Such "mass market" software products are those which (i) are distributed through retail distribution channels (including electronic transactions over the internet); (ii) include a cryptographic functionality that is not user-accessible and cannot be easily changed by the user; and (iii) are designed for installation and use by the user without substantial support from the supplier (i.e., "plug and play"). An exporter may treat a particular encryption software product as a "mass market" product only if that exporter has obtained an export classification ruling (called a "CCATS") from the Bureau of Industry and Security confirming that the product meets the "mass market" criteria, and is properly classified for export control purposes under ECCN 5D992, in accordance with section 742.15(b)(1) of the EAR.

There is a great deal of software, including open source software, that is freely available for download without restriction from the internet. Such freely available software may be excluded from the export controls described in this paper. Thus, section 734.3(b)(3) of the EAR provides that "publicly available" technology and software is not subject to the EAR. Under section 734.2(a)(1) of the EAR:

Items and activities that are not subject to the EAR are outside the regulatory jurisdiction of the EAR and are not affected by these regulations.

It should be emphasized, however, that that exclusion for "publicly available technology and software": does not apply to (i) encryption software classified under ECCN 5D002; or (ii) mass market encryption software classified under ECCN 5D992. Accordingly, the software supplier that proposes to make software products with encryption functions or features available for download from an internet site

---

6 Section 740.17 of the EAR establishes license exception ENC, which authorizes the export and reexport, without export licenses, of software products with encryption functions or features classified under ECCN 5D002. In order to utilize that license exception ENC as authority for the export or reexport of a particular encryption software product, however, the product must undergo "one time technical review" by the Bureau of Industry and Security, in accordance with section 740.17(d) of the EAR.
without restriction, even at no charge to the end-user, will be required to satisfy the following export compliance steps with respect to that encryption software:

a. Assuring that the software products are authorized for export. Generally, encryption software that is available for download from an internet site will meet the "mass market" criteria of the Cryptography Note in the Commerce Control List, supra. As explained above, however, under section 742.15(b)(1) of the EAR before that "mass market" encryption software product may be made available for download by persons located outside of the United States or Canada, a CCATS export classification ruling for the software product must be obtained from the Bureau of Industry and Security, confirming that the product does, in fact, meet the "mass market" criteria.

b. Unless the software products are made available for download on an anonymous basis, taking steps to assure that the products will not be: (i) downloaded to a location in an embargoed country; (ii) downloaded by, or made available to, a person or entity listed on one of the United States Government's lists of prohibited and restricted parties; or (iii) used in activities related to the proliferation of weapons of mass destruction ("WMD").

4. Specific Internet Software Export Transactions: Export Compliance Obligations

Based on the provisions of the EAR outlined in the preceding Sections of this paper, each of the following categories of internet software export transactions carries with it important export compliance responsibilities for the software supplier, and, given the nature of the internet, export compliance challenges for the supplier that may not arise in transactions in which tangible items (i.e., carrier media) embodying the software are physically shipped by the supplier to the foreign customer.

a. Electronic Fulfillment of Software Licensing Transaction: In this category of software transaction, the software supplier negotiates a software license agreement directly with each of its customers. For the convenience of the parties, and to minimize costs (e.g., shipping costs, customs duties, if applicable, etc.), once the software license agreement has been concluded, the software supplier then transmits the software over the internet from the supplier's server to the customer's computer. If the customer is located outside of the United States, the transmission of that software from the supplier's server (located in the United States) constitutes an export of that software under section 734.2(b)(1) of the EAR, supra ("export" includes transmission of items subject to the EAR out of the United States). For such an electronic software transmission, therefore, the software supplier must fulfill the following export compliance responsibilities:

---

7 On September 11, 2009, the Bureau of Industry and Security issued an advisory opinion which provides that a software supplier that makes mass market encryption software available for download from an internet site on a free and anonymous basis would not be subject to these end-user and end-use compliance requirements. If, however, the software supplier collects information about the end-user, such as user name and E-mail address, then the download transaction would not be considered anonymous, and the software supplier would be deemed to be in violation of the EAR if the software were downloaded to an embargoed country or by a prohibited or restricted person or entity. See BIS Advisory Opinion, September 11, 2009, available at www.bis.doc.gov/policiesandregulations/advisoryopinions.htm.
• As the "exporter", the supplier must assure that the software is authorized for export to the destination in question under authority of NLR, an export license exception, or an export license issued by the Bureau of Industry and Security. As the software in this type of commercial transaction is typically not publicly available without restriction, and is not furnished on a no charge basis to the customer, the software will not meet the requirements of section 734.3(b)(3) of the EAR. To the contrary, the software product will be "subject to the EAR" within the meaning of section 734.3(a) of the EAR. Moreover, if the software product in question includes data encryption functionality, and if the software is supplied to customers on the basis of individual license agreements, the product will most likely not qualify as a "mass market" encryption item. As such, it will be necessary to qualify that encryption software product for eligibility for export under authority of license exception ENC, through a "one time technical review" by the Bureau of Industry and Security, in accordance with section 740.17(d) of the EAR.8

• Section 740.17(b)(2) of the EAR identifies certain categories of encryption products (e.g., network infrastructure commodities and software; encryption software in source code form, other than open source; etc.) that are "restricted" for purposes of license exception ENC. Even after such "restricted" encryption products have undergone "one time technical review" by the Bureau of Industry and Security, in order to be qualified for export under license exception ENC, those "restricted" encryption products may not be exported, reexported or transferred within a single country to any "government end-user" unless it is located in one of the countries listed in Supplement No. 3 to Part 740 of the EAR.9 An export license from the Bureau of Industry and Security is required to provide any such "restricted" encryption product to any "government end-user" in any non-Supplement No. 3 country. Accordingly, if the software supplier's products have been classified by the Bureau of Industry and Security as "restricted" encryption products within the meaning of section 740.17(b)(2) of the EAR, the supplier must determine if its customer (located in a non-Supplement No. 3 country) is a "government end-user" within the meaning of the definition set forth in section 772.1 of the EAR, before transmitting or making those software products available to that customer.

• As the software supplier knows the identity (and, presumably, the location) of each individual customer, the supplier must take all appropriate steps to assure that the software is not transmitted to, or made available to, a customer that: (i) is located in a prohibited destination; (ii) is listed on one of the lists of prohibited and restricted parties; or (iii) will use the software in connection with a WMD proliferation end-use. To that end, the software supplier should take the following compliance steps before concluding the software license agreement with, and transmitting the software to, the prospective foreign customer:

---

8 Principal differences between the export compliance obligations applicable to mass market encryption software products classified under ECCN 5D992, and other encryption software products classified under ECCN 5D002 that have been qualified for export without export licenses under license exception ENC include: (i) the requirement under section 740.17(b)(2) of the EAR to obtain export licenses in order to supply "restricted" ECCN 5D002 software to "government end-users" in certain countries; and (ii) the requirement of section 740.17(e) of the EAR that exports of ECCN 5D002 under license exception ENC must be reported to the Bureau of Industry and Security on a semi-annual basis.

9 The Supplement No.3 countries include: (i) Canada; (ii) all 27 member states of the European Union; (iii) other European members of NATO (i.e. Norway, Iceland and Turkey); (iv) Switzerland; (v) Australia; (vi) New Zealand; and (vii) Japan.
(i) Confirm that the customer is not located in, and will not transfer the software to any person or entity, located in, an embargoed country.

(ii) Screen the customer (and any other party to the software licensing transaction) against the various United States Government lists of prohibited and restricted parties. If there is a suspected "hit" in that screening process, then the software supplier should not proceed with the transaction unless that "hit is verified as a false positive, or an export license for the proposed transaction is obtained.10

(iii) Obtain an end-use statement from the customer. That end-use statement should ideally include both: (a) an affirmative statement of the customer's intended end-use of the software product; and (b) the customer's covenant and undertaking that the software product will not be used, or made available to a third party for use, in activities directly or indirectly related to WMD proliferation.

b. **Sale of Software Applications through On-Line Stores**: In the past two years, led by Apple's enormously successful App Store, there has been tremendous growth and proliferation of on-line stores selling software applications for use on mobile telephones and other handheld devices.11 Under the typical on-line store model, the entity operating the on-line store authorizes third parties to develop software applications for distribution through the on-line store, and the operator then makes those third party software applications available for purchase by customers through the on-line store. To that end, the customer registers to use the on-line store, typically by providing the operator with his/her name, credit or debit card number and E-mail address, and by accepting the operator's terms of use. The customer is then granted access to a menu that identifies that software applications available through the on-line store, and may select, purchase and download the software applications that he/she wishes to acquire. In acquiring a particular software application, the customer may be required to accept, and agree to the terms and conditions of, an end-user license agreement (EULA) that states that the software application is licensed to the customer directly by the software developer.

Under the definition of an "export" set forth in section 734.2(b)(1) of the EAR, supra, if the on-line store operator's server is located in the United States, an "export" of a software application occurs whenever that software application is downloaded by a customer to a location outside of the United States. Even if the software application was originally developed abroad, once it is loaded onto the on-line store operator's server in the United States, the software application becomes "subject to the EAR" for United States export control purposes under section 734.3(a)(1) of the EAR, so that a subsequent download of that software application by a customer located outside of the United States is subject to the full range of United States export compliance requirements and restrictions.

---

10 In most instances, if a person or entity appears on one of the lists of prohibited and restricted parties, any application for an export license to supply items subject to the EAR to that person or entity will be summarily rejected. Export licenses may, however, be granted on a case-by-case basis for the export or reexport of non-sensitive items subject to the EAR to certain entities listed on the Commerce Department's Entity List, published as Supplement No. 4 to Part 744 of the EAR.

11 That on-line software application business already generates revenues for software application providers in excess of $1 billion, and the business is expected to grow to at least $4 billion by 2012. See *Business Week*, “The App Economy” (November 2, 2009).
As noted above, the party to any export transaction with primary responsibility for assuring compliance with the requirements of the EAR applicable to that transaction is the "exporter". In the on-line store model, there may be some uncertainty as to which of the several parties to any software application download transaction is the "exporter" of that software application, in the sense that: (i) the developer has developed the software, has furnished the software application to the on-line store operator for international distribution, and is deemed, as least as a contractual matter, to be licensing the software directly to the customer; (ii) the on-line store operator is the party that makes the software application available for download, controls the software application acquisition and download transaction, and has visibility as to the identity of the customer, but may not have information about the content or technical features of the software application; and (iii) the customer is the party that actually initiates the download of the software from a server in the United States to a foreign location. Nonetheless, in view of the definition of the term "exporter" in section 772.1 of the EAR, the on-line store operator should be treated as the "exporter", as the party in the United States with authority for controlling the transmission or download of the software application to a location or person outside of the United States. As such, the operator of an on-line software application store will have the following export compliance responsibilities:

- Confirming that each software application is authorized for export in accordance with the requirements of the EAR. To that end, the on-line store operator will have to rely upon information provided by the various software application developers, as those third party developers will be the only parties with detailed knowledge of the content of their software applications. At a minimum, therefore, the on-line store operator should require each developer to certify that his/her software applications are duly authorized for export in accordance with the requirements of the EAR. Moreover, as a matter of "best practice", the operator should also require each developer to certify that its software application does not contain or support of any data encryption functionality or features, or, if there is any such encryption function or feature, the developer should be required to furnish to the operator a copy of the CCATS export classification ruling from the Bureau of Industry and Security confirming that that software application meets the criteria for "mass market" encryption items, and is properly classified for export control purposes under ECCN 5D992.

- Taking steps to assure that no on-line store customer is located in an embargoed country. To that end, the on-line store operator should, at a minimum take the following three compliance steps. First, to the extent that a customer must complete a registration form in order to purchase software applications through the on-line store, the menu for entering the customer's address should not have entries for, and the registration form should not accept, any address located in an embargoed country (i.e., Cuba, Iran, North Korea, Sudan or Syria). Second, the on-line store operator should implement an "IP blocker" so that a person with an internet address in or associated with an embargoed country (e.g., .cu; .ir; .nk; .su; .sy) simply cannot access the on-line store website. Third, in agreeing to the on-line store terms of use, the customer should acknowledge that the on-line store may not be accessed or used by any person located in an embargoed country, and should certify that

---

12 Because on-line store operators typically require customers to register to use the on-line store, and typically request that customers provide at least a name, E-mail address and a valid credit or debit card number, those on-line store operators would not be able to rely upon the provisions of the September 11, 2009 Bureau of Industry and Security advisory opinion, supra, with respect to downloads by persons located in embargoed countries.
he/she is not located in, or a citizen or resident of, any such embargoed country.

- Taking steps to prevent access to the on-line store by any person or entity included on any of the United States Government's lists of prohibited and restricted parties. Again, there are at least three compliance steps that the on-line store operator should take to minimize the risk that software applications will be downloaded by a prohibited or restricted party, as follows. First, at the time that a prospective customer seeks to register to use the on-line store, the operator should screen that prospective customer against the various lists of prohibited and restricted parties. If there is, in fact, a "hit" against one of those lists, the registration application should be rejected, and the prospective customer should be denied access to the on-line store. Second, in agreeing to the on-line store terms of use, the customer should acknowledge that the on-line store may not be accessed or used by any person or entity listed on any of the United States Government's lists of prohibited and restricted parties, and the customer should certify that he/she is not included on any of those lists. Third, because the various lists of prohibited and restricted parties change frequently, the on-line store operator should periodically screen its entire customer database against the updated lists of prohibited and restricted parties, in order to confirm that no existing customer has been added to one of those lists after he/she registered to use the on-line store.\(^{13}\)

- Taking steps to prevent the use of software applications in WMD proliferation activities. This may be the most difficult of the export compliance responsibilities to fulfill in the on-line store context, because the on-line store operator may have no way in which to monitor or verify the end-users' actual use of the various software applications. At a minimum, however, the customer should be required to agree, in the on-line store terms of use and in each EULA, that any software application acquired by the customer through the on-line store will not be used, or made available to a third party for use, in any activities directly or indirectly related to WMD proliferation activities. The inclusion of such a provision in the terms of use and in each EULA may negate "knowledge" on the part of the on-line store operator that the software applications are intended for use by the customer in such prohibited end-uses.\(^{14}\)

c. **Software as a Service or Cloud Computing:** In recent years, various software developers and suppliers have developed or adopted business models variously described as "software-as-a-service" or "cloud computing". Under those business models, the customer subscribes to a service, which allows the customer to access and use the computational capacity of, and certain pre-determined software programs resident on, the service provider's servers. The customer

---

\(^{13}\) The foregoing steps are not, of course, "fool proof", but implementation of those steps should demonstrate good faith on the part of the on-line store operator to assure compliance with end-user restrictions in the EAR, and are consistent with the access control provisions listed in section 734.2(b)(9)(ii) of the EAR.

\(^{14}\) Under the non-proliferation provisions of sections 744.2, 744.3 and 744.4 of the EAR, an export license is required for the export even of otherwise decontrolled items if, at the time of export, the exporter knows (or has reason to know) that the items will be used directly or indirectly in the design, development, production, stockpiling, testing or use of nuclear, chemical or biological weapons or missiles. Those non-proliferation restrictions apply to exports to almost all countries with respect to nuclear weapons end-uses, to those countries listed in Country Group D:3 with respect to chemical and biological weapons end-uses, and to those countries listed in Country Group D:4 with respect to missiles. The various "Country Groups" for export control purposes are listed in Supplement No. 1 to Part 740 of the EAR.
may access those servers and software programs, and manipulate the customer's own data, by means of the internet. The attractiveness of the software-as-a-service or cloud computing business model is that it allows the customer to minimize its investment information technology infrastructure (computers, software, etc.), as it is able to use the service provider's infrastructure.

A key element of the software-as-a-service business model is that the customer does not purchase, and the service provider does not supply (either physically or electronically), complex software products to run on the customer's computers, the export compliance obligations applicable to this software as a service business model are frequently misunderstood. In a number of instances, United States-based service providers have erroneously concluded that they are not exporting any software, and therefore they have no compliance responsibilities under the EAR or other United States export control laws and regulations (e.g., the OFAC Economic Sanctions Regulations, infra). In fact, however, each United States-based software-as-a-service provider must be aware of, and must analyze how its business is affected by, the following compliance responsibilities.

- In many instances, it will be necessary for the customer to download certain software with the full range of export compliance responsibilities described in this paper (authorization for export, destination, end-user and end-use prohibitions and restrictions) in furnishing that software code to the customer\(^\text{15}\).

- By contrast, there may be circumstances, where the service provider does not provide any software code or other proprietary technology to the customer, or where all such software and technology is "publicly available" and is not, therefore, subject to the EAR under section 734.3(b)(3) thereof. In such circumstances, the software as a service transaction itself would not be subject to most of the provisions of the EAR\(^\text{16}\). That conclusion does not, however, imply that the service provider has no compliance responsibilities in providing its software as a service to its customers located outside of the United States. To the contrary, there are at least two sets of compliance concerns that must be addressed by the service provider, as follows:

(i) Section 744.6(a)(2) of the EAR provides that a United States person must obtain an export license from the Bureau of Industry and Security in order to perform "any contract, service or employment" which will directly assist in the proliferation of missiles in any Country Group D:4 country or the proliferation of chemical or biological weapons in any country worldwide. Section 744.6(a)(2) applies to the furnishing of any service by a United States person to a foreign customer, even when no commodities, software or technology subject to the EAR are involved in the transaction. The software as a service provider does, therefore,

\(^{15}\) Service providers should be aware of the provisions of section 7.42.15(b)(4) of the EAR governing the furnishing of code required to activate any latent encryption functionality of any software product. Under that section 742.15(b)(4), software code and components that allow an end-user to activate or enable the cryptographic functionality of other software products are treated for export control purposes as controlled encryption items.

have an obligation, in any event, to assure that its customers will not use the service in
furtherance of any such WMD proliferation activity.

(ii) The OFAC Economic Sanctions Regulations typically prohibit (a) the export or reexport of
any services from the United States to an embargoed country, or for the benefit of the
government of an embargoed country17; and (b) any transaction whatsoever in which a
person or entity on the OFAC list of specially designated nationals and blocked persons has
an interest18. In furtherance of its obligations under those OFAC Economic Sanctions
Regulations, the United States-based software as a service provider must confirm that its
customer is not located in an embargoed country, will not utilize the service for the benefit
of the government of an embargoed country, and is not listed on the OFAC list of specially
designated nationals and blocked persons19.

- In the ordinary course of using the service provider's services, a foreign customer may
upload and download data to the service provider's servers in the United States. To the
extent that any such data constitute "technology" within the meaning of section 772.1 of
the EAR, the download of those data from the server in the United States to the customer's
computer abroad will constitute an "export" of technology for United States export control
purposes. Nonetheless, in its January 13, 2009 advisory opinion, the Bureau of Industry
and Security concluded that the United States-based service provider would not be the
"exporter" of those data within the meaning of the definition of that term in section 772.1
of the EAR20. Accordingly, the United States-based service provider should not be liable
for violating the EAR in the event that some of the technology downloaded by the foreign
customer is controlled under the EAR, and would require an export license from the
Bureau of Industry and Security for export to the foreign customer's location.

- High performance computers are controlled for export under ECCN 4A003, but are
eligible for export or reexport to most foreign destinations under authority of license
exception APP, pursuant to section 740.7 of the EAR. Section 740.7(b)(2)(i) of the EAR,
however, provides that no Cuban, Iranian, North Korean, Sudanese or Syrian national may
have physical or computational access to any computer that falls within the scope of
license exception ENC21. In accordance with that section 740.7(b)(2)(i), as a matter of
"best practice" and out of an abundance of caution, the United States-based service
provider should include in its service agreement, especially with foreign customers, a
specific undertaking and covenant on the part of the customer to the effect that no national

---

17 See, e.g., sections 560.204 and 560.205 of the Iranian Transactions Regulations, 31 C.F.R. § 560.204, 560.204.
18 See, e.g., section 595.201 of the Terrorism Sanctions Regulations, 31 C.F.R. § 595.201.
19 The OFAC list of specially designated nationals and blocked persons may be found at www.treas.gov/offices/enforcement/ofac/sdn.
21 There is some ambiguity as to the scope of this prohibition on physical or computational access by nationals of embargoed countries.
The language of section 740.7(b)(2)(i) of the EAR prohibits access by those embargoed country nationals to any computer that is
"eligible for" license exception APP. That language implies that the prohibition applies even if the servers in question are located in
the United States. By contrast, the Bureau of Industry and Security's January 13, 2009 advisory opinion on software as a service and
cloud computing states that: "If a computer ... has been exported or reexported under License Exception APT ... then the access
restrictions will still apply, even if the computer ... will be used to provide a service that is not subject to the EAR."
of any such embargoed country will utilize the service or will otherwise seek to obtain access to the service provider's service. That provision should apply even if the servers that will be accessed by any particular foreign customer are located outside of the United States, if those servers were originally exported from the United States or are otherwise subject to the EAR.

5. Conclusion

As explained in this paper, export compliance responsibilities do not disappear simply because a software supplier uses electronic transmission over the internet as the means of delivering its products to its foreign customers, or because the supplier adopts a software-as-a-service business model. To the contrary, each time that a United States software supplier transmits or permits the download of any product or software code to or by a foreign customer, an export transaction occurs, to which the full range of export compliance requirements and restrictions mandated by the EAR apply. Even the furnishing of a service to foreign customers, under the software-as-a-service or cloud computing business model, implies compliance responsibilities on the part of a United States service provider, even if no software code or technology is provided to those foreign customers. The impersonal, remote and quasi-anonymous nature of many internet transactions may make it unusually difficult for a software supplier or service provider to fulfill those export compliance responsibilities, but any such software supplier or service provider will need to be in a position to demonstrate its compliance efforts, along the lines recommended in this paper, in order to avoid or mitigate severe export enforcement penalties, in the event that its software products or services are diverted to an unauthorized destination, end-user or end-use.
For more information:

John F. McKenzie
Partner, San Francisco/Palo Alto
+1 415 576 3033
john.mckenzie@bakermckenzie.com

Baker & McKenzie has been global since our inception. It is part of our DNA.

Our difference is the way we think, work and behave – we combine an instinctively global perspective with a genuinely multicultural approach, enabled by collaborative relationships and yielding practical, innovative advice. With 3,900 lawyers in 39 countries, we have deep understanding of the culture of business the world over and are able to bring the talent and experience needed to navigate complexity across practices and borders with ease.