CLOUD COMPUTING, EXPORT CONTROLS AND SANCTIONS

By Richard Tauwhare, Dechert LLP[i]

This is a summary of an article originally published in the August 2015 edition of The Journal of Internet Law and is reprinted with permission of Aspen Publishers

Introduction

Cloud services offer organisations in all sectors a wide range of potential benefits including the ability to use software from any device, to carry over files and settings to other devices seamlessly, to store, back-up and access data remotely, and in effect to lease the use of software or hardware instead of purchasing, maintaining, securing and upgrading it themselves.

By using these services, a user's data, software or technology may be routed through and stored in multiple countries to maximise server efficiency and data security, but often without the knowledge or intent of the user (except in the case of private clouds).

A key aspect of all such services is that they provide access *from* anywhere *to* data located anywhere. In doing so, they draw a rapidly-increasing number of organisations into conducting what are, in effect, cross-border transfers of information.

While the great majority of such transfers fall outside export controls and sanctions, nonetheless some will be prohibited or require a licence. Violations of these laws, though hard to detect, can attract heavy fines, imprisonment and reputational damage. Both cloud service users and providers need to be aware of whether and if so how the regulations apply to their activities.

This article offers an overview of the law, how it applies to cloud services users and service providers and what steps they can take to ensure compliance.

The Legal Framework: Purpose

Export restrictions may apply as part of the general controls on what may be exported (generically termed 'export controls') or as part of a regime of trade, travel and financial sanctions adopted in relation to a particular country, entity or individual. The two sets of laws have similar, over-lapping objectives:

- export control laws help to prevent the proliferation of Weapons of Mass Destruction (WMD) and the abuse of conventional weapons by governments or non-state actors;

- sanctions put economic pressure on governments, entities or individuals to change their policies and restrict their capacity to continue to pursue their current policies.

The Legal Framework: Penalties

Given the strategic importance of these controls, violations are a strict liability offence (ignorance is not an excuse) and the penalties can be severe. In the UK, enforcement action is led by HM Revenue and Customs and, as necessary, the Crown Prosecution Service. The penalties range from warning letters, revocation of existing licences, seizure of goods, fines and up to 10 years' imprisonment, compounded by serious reputational damage.

The US regulators are considerably more robust and exert extraterritorial jurisdiction in respect of many of their controls. EU individuals or organisations found to be in breach of the US laws can potentially be added to one of the US lists of Denied Parties (see more on these below). Since this in practice would put them out of business, such individuals or organisations generally prefer to pay a fine: in 2014, a French bank paid a fine of $9 billion for violating US sanctions on Sudan.

The Legal Framework: Export Controls

The following offers an overview of the main categories of controls and exemptions.

Dual Use

The items included in the dual-use lists, and therefore subject to controls, cover a wide range of fields including: nuclear engineering; biological sciences and pharmaceuticals; chemicals with toxic properties; high strength materials; high specification electronics, computers, and telecommunications; automation and control systems; lasers, optics and sonar; navigation and avionics; submersible equipment; aerospace; and – the main basis for controls on software – encryption.

End Use

The regulations also provide for 'end use' controls which are defined not on the basis of the exported item itself but on how it will ultimately be used. In the EU, there are two main categories of end-use which require a non-listed item to be licensed: if the exporter has been informed, is aware or has reason to suspect that it will be used for WMD purposes[ii] outside the EU; or if it may be intended for military use in a country subject to an arms embargo.

Intangible Transfers of Technology

The controls apply not only to goods but also to software and technology. Technology is defined as information useful for the development, production or use of controlled goods. Controlled transfers can include giving access to software or technology in electronic form to someone located overseas for example by uploading information to a server. This is considered further below.

Exemptions

The controls are not intended to interfere unduly with normal commercial or academic practices. As a result, there are a number of exemptions for the transfer of technology:

- Information 'already in the public domain'. This is defined as 'available without restriction upon further dissemination (no account being taken of restrictions arising solely from copyright)'. As an example, inclusion of information in a book, website or exhibition would be considered as 'public domain' but where there is restricted access such as registration needed to access the website, the item would no longer be 'public domain'. If the information has a security classification or requires a non-disclosure agreement, or if there are any other intellectual property restrictions, then the information is clearly not in the public domain and is not exempted;

- 'Basic scientific research'. This is defined as 'experimental or theoretical work undertaken principally to acquire knowledge of the fundamental principles or phenomena or observable facts and not primarily directed towards a specific practical aim or objective.' Research with potential commercial applications is unlikely to be exempt;

- technology that is the minimum necessary for installing, operating, maintaining and repairing controlled items that have already been authorised for export, or for non-military items. For example, a manual for the repair of a non-military turbojet engine might contain technology also required for the repair of a military turbojet engine. However, if the manual constitutes the minimum technology necessary for the repair of the non-military engine, it would not be classified as controlled technology;

- shared dual use technology. Similarly, technology which is shared between controlled and non-controlled dual use items is not controlled. For example, if a company wished to transfer technology for the production of a non-controlled metal alloy, if this was the same technology as that used for the production of a controlled metal alloy, then the technology is not controlled. Nuclear-related technology is not included in this exemption;

- the minimum necessary information for patent applications. Again, nuclear-related technology is not included.

These exemptions do not apply if there are WMD end-use concerns (except for transfers within the UK, by UK persons outside the EU or non-electronic transfers, if they concern information in the public domain).

Cryptography

One of the main categories of software subject to controls is that designed for information security[iii], particularly software designed or modified to use cryptography or to perform cryptanalytic functions. Given the rapid expansion of aggressive cyber attacks on both Government and private sector organisations, and the countervailing expansion of

information security solutions on the market and under development, Governments' concerns about the nature of dual-use items have evolved rapidly.

US Controls

Other major exporting countries impose similar controls, notably the US. But a significant difference in the US regulations, both for sensitive military items (ITAR)[iv] and for less sensitive military and all dual use items (EAR)[v], is that the controls apply not only to the original export of an item from the US but also to the subsequent transfer or re-export of that item, or of an item into which it has been incorporated, or items made using US-origin controlled technology.

The US definition of re-export includes the release *within the destination country* of controlled software and technology to a dual or foreign national from a country to which restrictions apply for the item (termed a 'deemed re-export'). US-controlled items therefore require particularly careful handling to avoid unintended, unauthorised re-exports, notwithstanding that this entails a significant stretching of the traditional notion of extraterritorial jurisdiction.

The Legal Framework: Sanctions

All UN member states are obliged to give effect to UN Security Council sanctions resolutions. But some, particularly the EU and US, commonly adopt further measures. Firms and individuals need to be aware not only of the EU measures (which apply to all EU persons and entities incorporated under the law of a Member State wherever they are located, as well as to anyone located in the EU) but also of which other countries' sanctions may apply. In particular, the US asserts a very broad jurisdiction for its sanctions.

Sanctions take a variety of forms but often involve some form of export control, including:

- embargoes on exporting weapons, equipment that might be used for internal repression, and associated technical assistance, training and financing;

- restrictions on dealing with named individuals or entities, or with entities which are more than 50% owned by (or, in the case of EU measures, 'controlled' by) named individuals or entities. Consolidated lists of sanctioned organisations and individuals ('Denied Parties') are compiled for the UK by HM Treasury[vi] and for the US by the Office for Foreign Assets Controls[vii]. Prohibited activities can include contracting with, selling to, shipping to, receiving payment from, making payment to, or conveying technology to such parties;

- bans on trade in specified categories of goods (e.g. dual use goods, oil and gas equipment) or services (e.g. financial transfers, insurance, investment, technical assistance), either to designated individuals and entities or to a whole country.

Application of these Laws to Cloud Users and Service Providers

Export controls

The key to demystifying the application of export controls to cloud computing lies in clarifying what is an 'export' and who is an 'exporter'. Although one of the US authorities with oversight of export controls has provided some guidance, the European Commission has not and there remains some lack of clarity on these points.

What is an export?

In the case of physical exports of goods, this is relatively straightforward to define and interpret: an item is transported to another country as determined by, or in fulfilment of a contract held by, the exporter.

In the case of intangible transfers of technology, the issue is less clear-cut. The definition of 'export' in the EU Dual Use Regulation includes '*transmission of software or technology by electronic media ... to a destination outside the EU; it includes making available in an electronic form such software and technology to natural and legal persons and partnerships outside the EU.*' This suggests that there are two acts, either of which constitutes an export:

a) making software or data available to any person physically located outside the EU;

b) transmitting software or data outside the EU.

In the case of (a) there is no dispute that an export does indeed occur, since the software or data comes into the possession of a person outside the EU who can then make use of it. This could involve the software or data being first transmitted and then accessed outside the EU. Or it could involve software or data that has not been transmitted overseas but is stored on a local server and then accessed by a person outside the EU. In either scenario, the result is the same. If the software or data is subject to export controls, both actions constitute an export and require a licence.

In the case of (b), however, this is not evident. Although the software or data have been transmitted across a border and are physically stored in electronic form outside the EU, if no one has access to their content then the opportunity to make use of them has not in fact been transferred to anyone. Whether a piece of EU-controlled data is located in a server in Scotland or Singapore is in itself irrelevant. What matters, from a practical perspective, is the location of those who can access that data. If access is effectively restricted to only people located in Scotland, then if the data is uploaded from Scotland to a server in Singapore and then downloaded back to Scotland, no export has taken place and no controls are engaged.

Guidance from the UK and US authorities appears to support this interpretation. The UK guidance is clear that transfers of data or software overseas are not controlled if no-one located outside the EU has access to it. It is only the act of *making controlled technology or software available to anyone outside the EU (or, in the case of military and Annex IV dual use*

controls, outside the UK), whether through a cloud service or indeed by any other means, that requires a licence.

This is reflected in the UK Government's guidance on the timing of when a licence is required in accessing controlled software or technology:

- if controlled software or technology is to be accessible to individuals or groups located outside the EU from the time when it is first saved to a site, then a licence is needed before it is saved to the site; but

- if individual permissions are required for individuals or groups located outside the EU before they can access the site, then it is only necessary to obtain an export licence before that permission is given.

Reinforcing this interpretation, the US Department of Commerce Bureau of Industry and Security (BIS) Advisory Opinions[viii] on the application of the Export Administration Regulations to cloud computing services confirm that permitting a foreign national to maintain a cloud service provider's servers and software does not constitute a "deemed export (or re-export)" to the foreign national's country of citizenship, provided that such foreign nationals do not have access to the user content. This indicates that it is *access to user content* that is required for an export or deemed export to be said to have taken place.

From this core understanding, a number of implications logically follow:

- **location of the data or software**: for the purpose of UK export controls, it is irrelevant where the software or technology itself is stored or routed, provided that adequate measures are in place to prevent unauthorized foreign nationals (e.g. system administrators) from having access to its content;

- **ownership of a server**: the controls apply irrespective of who owns the server on which controlled software or technology is made available, e.g. whether it is on an organisation's own servers or on those of any cloud service;

- **nationality**: the controls apply irrespective of the nationality of the person in the UK who makes the software or technology available and of the person given access to it outside the EU. The regulations apply not only to all EU but also to all non-EU persons conducting business in the EU;

- **employment status**: it makes no difference whether a transfer is 'internal' between staff of the same company located in different countries, or to a different entity. The controls apply irrespective of the employment status of either the uploading or the downloading person. They could be a UK member of staff travelling overseas, a member of staff of a subsidiary overseas, an established customer with access rights, or anyone else;

- **intention**: controls apply irrespective of whether or not a member of staff abroad with access to the software or technology has any intention of passing it on to another

person abroad. This corresponds to the rules for physical exports, where taking controlled technology abroad, even if only for personal use and not for onward transmission while abroad, still requires a licence.

Nonetheless, it is important to be aware that this interpretation of the EU regulations may not be applied in all countries. They may consider that the act of transmitting controlled software or technology out of their country, irrespective of who has access to it, may still render it subject to export control laws. This is an area of ambiguity that the relevant authorities would do well to clarify.

Who is an exporter?

Again, this is less clear for intangible transfers of technology than for physical exports of goods. The European Commission has not provided specific guidance on this. In the absence of such guidance, the key again appears to lie in the definition of 'exporter.' The EU Dual Use Regulation states that this includes any natural or legal person or partnership '*which decides to transmit or make software or technology by electronic media ... to a destination outside the Union*.'

On the basis of this definition, the exporter is the person who decides to grant access to controlled software or data to a person located outside the EU. In most cases this will be the cloud user rather than the service provider. Some argue that if a user uploads software or data to a cloud but the service provider, without the knowledge of the user, then moves that software or data to be stored in a server outside the EU, it is the service provider who is the exporter. But this does not take account of the interpretation set out above that the transmission of software or data out of the EU does not in itself constitute an export. Nor does it reflect the rules applicable to physical exports, for which it is the company holding the contract for an export, not the freight forwarder or shipper, who is responsible for securing a licence before any licensable activity may take place.

But there could be circumstances in which a cloud service provider decides to grants access to controlled software or data to a person located outside the EU, for example to a systems administrator. If they do so, they need to be aware that the licensing obligation then falls to them.

The US authorities appear to share this view, in two complementary ways. The BIS Advisory Opinions make clear that:

- cloud service providers are not themselves subject to export controls and do not have a responsibility for policing the activity of users on their servers, as long as they do not themselves initiate the export of controlled software or technology; and

- cloud service providers giving users access to Software-as-a-Service (SaaS) services are not conducting an export since the user does not download executable software but only makes use of software on a remote server.

However, this remains again an area of some ambiguity on which guidance from the EU authorities is overdue.

Export controls in sanctions programmes

Sanctions may apply if any software or technology is made available to a person or entity who is either:

- located in a country subject to sanctions and the export of the software or technology in question contravenes the terms of the embargo established by the sanctions (for example, if military technology is made available to a person located in a country under an arms embargo); or

- is themselves included on a list of sanctioned persons or entities, or they are owned or controlled by such persons or entities, and the provision of the software or technology to them contravenes the sanctions.

Such measures apply equally to service providers as well as users. Neither the US nor the EU authorities have published formal guidance on this aspect so organisations must interpret and apply each set of sanctions measures as they are drafted.

Steps to Ensure Compliance

The following offers some pointers for both users and providers of cloud services.

Compliance best practice

The compliance procedure needs first to determine whether an item is included on the military or dual use control lists (if in doubt, apply for a licence on a precautionary basis, at the risk of losing 3-4 weeks to be informed that no licence is required).

Secondly, consider whether an item is subject to end-use controls: these apply to any non-listed item if the exporter has been informed, is aware or has reason to suspect that it will be used for WMD purposes outside the EU, or if it may be intended for military use in a country subject to an arms embargo.

Third, determine whether an item is subject to US re-export controls. Ensure that the supplier provides detailed information on what controls apply to it and includes, in their US export licence, authorisation for any proposed re-exports. Put in place all measures necessary to ensure that the US control requirements are fully met.

Fourth, check whether any country, entity or person involved in a proposed transaction is subject to any applicable sanctions. This applies to cloud service providers as well as users, who should screen all users of their services, their partners and the locations of their servers and other facilities. Screening should be repeated regularly to take account of the frequent changes in the sanctions rules and lists.

If these steps determine that export controls or sanctions do apply to the provision or use of cloud services for certain software or data, the potential 'exporter' (as defined above) should consider whether to apply for a licence or to take steps to prevent the controlled software or data being placed in the cloud in a way which could breach the controls. The main steps include measures such as the following:

- establish robust procedures governing who has access to controlled software or data from outside the country;

- limit controlled software or technology to only private servers or to a private cloud in which the user determines the routing and location of storage;

- negotiate contracts with cloud service providers which:
    - restrict the routing and storage locations;
    - restrict access, including by system administrators. (EU regulators have not defined what they consider to be 'adequate' measures to prevent unauthorised access - this remains the exporter's responsibility[ix]);
    - restrict copying of controlled software or data by service providers and require that all copies are deleted when the cloud services are terminated;
    - give the user the right to audit the service provider's compliance;
    - oblige the provider to notify promptly any known or suspected breaches;
    - address the respective responsibilities of the parties for export compliance.

Licensing

If a cloud service or use is not prohibited by sanctions but is subject to export controls, the final step is to obtain and meet the conditions of an export licence. Depending on the proposed activity, this need not be unduly onerous.

Traceable records of all licensed activities must be retained as required by the licence so that queries about any transactions under licence may be readily checked and an adequate audit trail followed.

Conclusion

Using cloud computing services can create risks for those handling software or technology that is subject to export controls or whose transfer could breach sanctions. The key is to recognise that making software or technology available to anyone located outside the UK or EU, however this is done, may require a licence and could breach sanctions, so appropriate procedures need to be put in place to manage the risks.

---

[i] Richard Tauwhare is a Senior Director in the London office of Dechert LLP, a global law firm. He specialises in advice on ensuring compliance with export controls and sanctions. He was formerly head of export controls policy in the Foreign and Commonwealth Office.

[ii] 'WMD purposes' are defined by the Export Control Order 2008 as '*use in connection with the development, production, handling, operation, maintenance, storage, detection, identification or dissemination of chemical, biological or nuclear weapons or other nuclear explosive devices, or the development, production, maintenance or storage of missiles capable of delivery such weapons*.' The definition is also understood to include large Unmanned Aerial Vehicles, which can also be capable of delivering such weapons.

[iii] Category 5, Part 2 of Annex I of the EU Dual Use Regulation

[iv] The International Traffic in Arms Regulations, administered by the US Department of State

[v] The Export Administration Regulations, administered by the US Department of Commerce

[vi] HM Treasury's Consolidated List of Financial Sanctions: https://www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases

[vii] OFAC's Consolidated Sanctions List: http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/consolidated.aspx

[viii] US Bureau of Industry and Security Advisory Opinions: https://www.bis.doc.gov/index.php/policy-guidance/advisory-opinions

[ix] One option is to encrypt the technology. There is no EU guidance on this but the US authorities have not accepted that encrypting technology to established US government standards gives adequate protection to controlled technology, except if access is limited to US persons abroad who are directly employed by the same US corporation that sent the technology and the technology can only be used by US persons.