LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Export Controls, Economic Sanctions & Customs Practice

October 23, 2014 | Number 1761

5 Compliance "Hot Spots" for Technology Companies Under Export Controls and Sanctions Laws

Increasingly interconnected global businesses need to focus on how export controls and trade sanctions can affect their cross-border activities in unexpected ways.

For decades, the US Government has used trade controls — export controls as well as trade and economic sanctions — to advance national security and foreign policy interests. These rules, many of which have not kept pace with rapid advances in technology, create significant compliance challenges for companies and individuals around the world.

At their core, US trade controls apply restrictions on transfers of sensitive products, software, and technology, as well as dealings with certain countries, governments and specified parties. For technology companies, compliance challenges are most significant when dealing with either sensitive technologies, third parties whose identities and locations are difficult to ascertain, or both. This alert addresses five compliance "hot-spots" for technology companies under US trade controls.

1. Web-based Interactions with Customers and Other Third Parties

Conducting business online offers tremendous business benefits in the form of new customers, suppliers and partners around the world, but it can also lead to trade controls compliance challenges. Companies with a significant Web presence (for example, e-commerce companies, companies that provide services online and social media companies) may reach millions of potential customers and business partners, the identities or even existence of which may be unknown to the company.

Applicable trade controls, however, carry an expectation that companies "know their customers" and can impose strict liability for dealings with sanctioned or denied parties. The U.S. Treasury Department's Office of Foreign Assets Control (OFAC), which administers and enforces most US sanctions, offers the following general guidance: "[f]irms that facilitate or engage in e-commerce should do their best to know their customers directly." OFAC FAQ No. 73.

In response, many companies have implemented screening systems and other safeguards designed to ensure compliance — even in business environments that the relevant legal regimes have not yet fully addressed. Examples include screening counterparties to avoid transactions with parties that are the targets of US sanctions (*e.g.,* through IP address blocking software designed to identify IP addresses associated with an embargoed country) and requiring counterparties to enter into terms of use that certify compliance with applicable trade controls.

2. Cloud Computing

"Software-as-a-service" (SAAS) or "cloud computing" business models have exploded in popularity. These business models allow SAAS customers to access and use an SAAS provider's servers rather than invest in their own technology infrastructure. SAAS business models present particular compliance challenges, complicated in part because the applicable regulatory frameworks may carry different requirements for different parties.

For example, the U.S. Department of Commerce's Bureau of Industry and Security (BIS), which administers the Export Administration Regulations (EAR) covering exports and reexports of civil, dual-use, and some military items, takes the position that SAAS providers are not "exporters." However, the SAAS customers who upload EAR-controlled technology to cloud-based servers may be treated as exporters in certain circumstances, such as when the servers are located outside of the United States or the technology is accessible to non-US persons. This interpretation provides some relief for SAAS providers in the context of the so-called "deemed export" rule, which treats releases of technology and certain software to non-US persons (*i.e.*, individuals who are not US citizens, US lawful permanent residents, or otherwise part of a narrow protected class such as asylees) as exports to those persons' countries of nationality, even if the transfer occurs wholly within the United States.

Indeed, BIS has similarly stated that because SAAS providers are not "exporters," they do not cause a "deemed export" when their foreign national administrators access user-generated technology subject to the EAR. The deemed export rule nonetheless requires, however, that SAAS providers take steps to protect their export-controlled software and technology against unauthorized access by non-US persons, whether located in the United States or abroad. Similarly, customers of cloud-based services platforms must also take steps to ensure that their use of such services complies with applicable export control requirements, including ensuring that controlled technology is not exported or reexported or otherwise made accessible to non-US persons without proper authorization.

OFAC has not issued guidance drawing the same distinction between SAAS providers and customers. Absent such guidance, OFAC's traditional "know your customer" concept must be taken to apply equally in the cloud computing space. Therefore, both SAAS providers and customers should consider whether restricted party screening and other safeguards may be necessary to ensure that those accessing cloud-based services are not targets of US sanctions.

3. Encryption

Software that contains encryption functionality is often subject to some degree of export control restriction, the level of which turns on the purpose and strength of the encryption. The EAR carve out from more strict controls items incorporating or using cryptography whose "primary function or set of functions" is not "information security," computing, sending, receiving, or storing information, or networking. The carve out also exempts from control cryptographic functionality that is limited to supporting these primary functions or sets of functions.

Other exceptions include:

- Encryption technology used solely for user authentication, password protection, or other forms of access control
- Software that uses a weak encryption functionality (*i.e.*, encryption using a key length of less than 56 bits symmetric, 512 bits asymmetric, or 112 bits elliptic curve)

- Certain “mass market” encryption software products

- Certain open source software that is available for free and anonymous download from the internet (note that the download of software from sites requiring users to “register” by providing certain identifying information is not considered anonymous and thus may result in violations where persons in sanctioned countries make downloads)

Even to the extent, however, that encryption software falls within one of these narrow exceptions, such software may nonetheless be subject to other regulatory requirements relating to company registration with BIS, formal export classification rulings, and annual or semi-annual reporting of export sales. Accordingly, companies that deal in encryption software— or whose products rely on third-party products for encryption functionality — should take steps to export-classify their products, an analysis that typically requires input from both technical and legal personnel.

4. Shared Networks

Shared networks can facilitate business requiring the participation of highly skilled personnel located both in the United States and across the globe. However, these platforms also present inherent trade controls risks. For purposes of compliance with the deemed export rule, technology companies may need to restrict certain technology from access — or, in the case of ITAR-controlled technical data, *potential* access, even if such access never actually occurred — by non-US persons, or otherwise secure export authorization under the EAR or the ITAR.

Relatedly, for certain categories of visa applicants, the I-129 Application for Nonimmigrant Workers (*e.g.*, H-1B status application) requires employers to certify in writing whether the foreign national employee being sponsored will have access to export-controlled technology subject to EAR or ITAR licensing requirements.

5. Mobile Devices and the International Traveller

The demand to stay constantly connected can create trade controls risks for international business travelers. In some circumstances, US regulations may restrict or prohibit exports of controlled technology residing on (and accessible through) a traveler’s laptop or mobile device, and the device itself. At the same time, there may be limited regulatory exceptions permitting hand-carrying of items and the export of services, software and hardware used for personal communication (*e.g.*, social media services and smartphones). *See,* for example, EAR Exceptions for Temporary Imports, Exports, Reexports, and In-Country Transfers and for Baggage.

Businesses (and business travelers) should recognize that these limited exceptions may not extend to controlled technology and services unrelated to the exchange of personal communications (for example, the controlled technical data that a business traveler may store on a laptop) or business-related communications conducted through a personal communication device while traveling in a sanctioned country. As an added challenge, the rules may vary depending upon the country at issue.

Technology companies should take steps to ensure that their employees are aware of where they can and cannot take their work and tools of trade — whether they are traveling for business or pleasure.

Conclusion

While new technologies bring with them increasing opportunities for global connectedness, long-standing rules and regulations restricting exports and trade will continue to create potential, sometimes unexpected

risks for those operating in the new business landscape. Companies operating across borders — whether through third parties, customers, or their own employees — should take precautions to ensure that they remain compliant with export controls and trade sanctions.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Annie E. S. Froehlich
annie.froehlich@lw.com
+1.202.637.2375
Washington, D.C.

Scott C. Jones
scott.jones@lw.com
+1.202.637.3316
Washington, D.C.

Les P. Carnegie
les.carnegie@lw.com
+1.202.637.1096
Washington, D.C.

Kevin P. DiBartolo
kevin.dibartolo@lw.com
+1.202.637.2290
Washington, D.C.

William M. McGlone
william.mcglone@lw.com
+1.202.637.2202
Washington, D.C.

You Might Also Be Interested In

Ukraine Crisis Update: US and EU Expand and Align Sanctions

A Changing Landscape for U.S. Importers of Defense Articles

Risk Assessments: Avoiding Trouble in Emerging Markets

Managing Legal and Business Risks Under the Russia/Ukraine Sanctions: Views from the US, Europe and Moscow