

Understanding U.S. Export Controls for Internet Based Products

The United States maintains one of the world's most comprehensive set of laws and regulations governing the export of technology. These laws apply to "traditional" exports – such as a widget going from Maryland to Mexico - as well as "electronic" exports – such as a person from Mexico viewing a website from his house in Mexico City. It is imperative that on-line companies keep the last example firmly in mind when analyzing their compliance efforts. When your web site, or your customer's web site, is accessed from outside the United States an export has occurred. When analyzing this issue, it is easy to use the analogy that you have caused your server to export data to a computer outside the United States.

All exports are subject generally to certain U.S. Department of Commerce restrictions, and other controls, such as the U.S. embargo of Cuba and the Foreign Corrupt Practices Act, which are administered by other agencies. While many U.S. government agencies possess jurisdiction over the export of some items, most items which are subject to export restrictions, fall within the jurisdiction of either Department of Commerce's Bureau of Export Administration or U.S. Department of State's Office of Defense Trade Controls. With the exception of certain transaction based controls, and embargoes, most other export licensing regulations are sector specific.

The following is an overview of key U.S. laws which pertain to products accessed or deployed over the internet.

Department of Commerce

The Export of many items is regulated by the Department of Commerce - Bureau of Export Administration (Commerce), pursuant to the Export Administration Act and Regulations. The Export Administration Act has expired. However the Regulations have been subject to "emergency" extensions for over five years. As a

result, only the Regulations are currently being enforced by Commerce.

Commerce assesses the risks associated with exports by classifying a product based on its ultimate destination and principal characteristics. Software and technology that may not be accessed by someone from a foreign country would be set out on the Commerce Control List (CCL). The CCL classifies products based on their essential characteristics.

In order to determine if the exporter of a product or commodity requires an export license, a company must evaluate the country of ultimate destination and essential characteristics of type of product to be exported. From that analysis, a determination can be made whether the export requires a license, and if so, the type of license required. Items for which licenses are required include particular types of software and other technology products. Again, it is important to understand that if your customer accesses your server from a foreign country – an export has occurred – regardless of the fact that the server is in the United States.

Penalties for violation of Commerce regulations can be severe and may lead to criminal prosecution against corporate officers and officials, arrest, and monetary penalties. Penalties for either the principal offender, or an entity determined to have facilitated the violation may be:

- 10 years imprisonment for violations of export regulations controlled for foreign policy purposes;
- \$1,000,000 per violation for transgressions involving U.S. national security;
- \$50,000 per violation for other export violations;
- Denial of export licenses on an unlimited and company-wide basis; and
- Seizure of the products and vessels involved in the unauthorized transaction.

Department Of Treasury

The President has been given the authority to impose restrictions on international transactions by executive order. The Department of Treasury's Office of Foreign Assets Control (OFAC) administers these orders. The economic prohibitions and sanctions may be wide ranging and can often prohibit persons and companies subject to U.S. jurisdiction from engaging in almost any type of business activity with designated countries, their nationals or certain individuals.

For companies doing business over the internet, the most important set of restrictions is set out on the Specially Designated Nationals list ("SDN list"). The SDN list contains over 127 pages of individuals and organizations with whom U.S. companies may not do business. For example, you may not host a web site for an entity, such as Hezbollah, which is set out on the SDN list. The fact that you do not know you are hosting a site operated by an entity set out on the SDN list, will not necessarily insulate you from liability under the law.

Penalties for violation of the laws authorizing the President's Executive Orders have included civil fines of up to \$300,000.

Other Laws and Departments

The two departments set out above administer programs that most directly affect companies doing business over the internet. Depending on your business, you may also be subject to laws administered by the Departments of State and Defense. You should also be aware that all U.S. companies are required to abide by the Foreign Corrupt Practices Act and the Anti-boycott Act, as well as other acts, such as the Cuban Democracy Act which have specialized application.

Effective Compliance Programs

Each industry involved in exporting should have an export compliance plan designed to the unique needs of its business. For companies like yours, these plans should include:

- ✓ Screening all new customers against the SDN list;
- ✓ Reviewing all software and technology that may be accessed by customers and, if applicable, visitors to customer sites using your technology, to determine if it is present on the CCL;
- ✓ Training customer support and sales staff on relevant regulations governing who, and which countries, U.S. companies may not do business;
- ✓ Regularly updating compliance programs to ensure recent changes to lists and laws are incorporated.

The above discussion is intended merely as a general summary of the relevant law for background purposes. It is based on an analysis of relevant law as of October 2003. Laws change, administrative agencies issue guidelines, and courts make rulings – please consult with your attorney before making decisions based on this article.

David Snead is an attorney in private practice in Washington D.C. His practice focuses primarily on representing web hosting providers, ISPs, and other entities involved in the dissemination of content and provision of services over the internet. In his 10 years in this area, Mr. Snead has represented ISPs, web hosts, and telecommunications providers both in-house and as outside counsel. Mr. Snead received his J.D. in 1991 from Georgetown University Law Center and is a member of the bars of the District of Columbia and State of New Mexico.