8/29/2001

U.S. EXPORT CONTROLS ON TECHNOLOGY TRANSFERS

Companies selling technology products abroad must be careful that they have complied with regulations imposed on the exportation of technology products. This is especially true for companies seeking to export encryption technology. This iBrief explores the considerations that must be given to the export of encryption and other technologies.

¶ 1 When a company sells its products or allows its products to be sold in a foreign country it must first determine whether the U.S. Government has placed any controls on the transfer or export of any technology used in that product. The Commerce Department's Bureau of Export Administration ("BXA") administers non-defense and dual-use products (military and commercial use).[1] The guidelines for exporting these products are set forth in the Export Administration Regulations ("EAR").[2] Companies may export most types of technology, including software and other computer products, by checking the export control list and claiming a general license. However, certain technologies are subject to export controls and companies that export them without a license can face fines and other penalties.

¶ 2 Currently, the standards for exporting sensitive technologies are the subject of much debate. For example, although encryption technology has numerous commercial uses, the potential for its use in military settings has prompted concern by the U.S. State Department, which sought to restrict exports.[3] At the same time, companies concerned about their bottom lines and foreign competition have pressured Congress and the President to loosen export controls on technology.[4] In 1996, President Clinton transferred licensing decisions over encryption technology to the Department of Commerce.[5] Some commentators have argued that, since the Commerce Department favors exports, this has resulted in relaxed export controls over sensitive technologies.[6] However, exporters who wish to sell encryption technologies abroad, for example, still face a number of potential obstacles.

¶ 3 A crucial determination for an exporter is whether its products use encryption technology since certain technologies for encryption cannot be transferred outside the United States.[7] Companies can export most non-encryption software to most countries without an export license. The major exception to this general rule involves transfers to countries such as Cuba, Iraq, Iran, Libya, Sudan, Syria and North Korea that are subject to sanctions or other

export controls.

¶ 4 Conversely, the EAR treats products containing certain types of encryption technology differently. Many companies may be surprised to find that the EAR may deem many types of seemingly routine activities, such as use of the Internet or visits by scientists with foreign citizenship, exports of technology. For instance, under EAR section 734.2(b)(9) merely posting encryption software on the Internet can be an "export" for the purposes of the regulation.[8] However, if companies take sufficient precautions against unauthorized transfers then they may avoid falling within the EAR's definition of "export." These precautions include ensuring that access to the software is restricted to systems with United States addresses and requiring that a receiving party "affirmatively acknowledge" that he or she understands that the cryptographic software is subject to export controls.[9]

¶ 5 Additionally, the BXA views technology as "released for export" whenever it is visually inspected by foreign nationals or whenever there is an oral exchange of information concerning the technology, whether in the U.S. or abroad. Likewise, an export occurs when employees, having obtained personal knowledge or technical experience regarding encryption in the United States, apply that knowledge or experience abroad.[10] Suppose a foreign scientist visits a U.S. manufacturer for encryption devices using a technology that cannot be exported. The scientist is allowed to visit the factory where the encryption is manufactured. Under the current regulation this would be a prohibited technology transfer and the company could face fines and charges unless it first obtained a valid export license.[11] Additionally, suppose the President of the Company gives a speech at a technology conference overseas, giving the details of the encryption technology. This also would be a prohibited transfer or export that could subject the company to penalties.

¶ 6 Companies may also run into problems using controlled technology in their foreign subsidiaries. As a consequence of the "Deemed Re-export Rule," any release of technology or source code to a foreign national *in a foreign country* is considered a re-export to the home country of that foreign national.[12] Thus, companies with foreign subsidiaries should be careful to ensure that, even if the foreign subsidiary has the proper license and permission to use the technology, the company does not unintentionally export the technology to a third country and face penalties.

¶ 7 United States companies that sell encryption technology or products that use encryption technology may find themselves at odds with these controls. United States companies

that sell products with encryption technologies face increasing competition from foreign companies whose governments have not placed strict controls on the transfer of technology. Specifically, the creation of the free-trade zone among members of the European Union allows those countries to transfer freely those technologies among themselves. To address this problem, the BXA released new rules for exports, allowing the export of encryption products to 15 members of the EU and 8 additional trading partners.[13]

¶ 8 In addition to lobbying the government to change export control policy, companies have disputed the government's attempts to regulate encryption technologies on the grounds that the source codes for encryption technologies is speech protected by the First Amendment. For example in Bernstein v. U.S. Dep't of Justice, a three judge panel of the 9th Circuit recognized that the First Amendment protected encryption source code since it was the best means to express cryptographic ideas and algorithms.[14]

¶ 9 In another important case, Peter Junger, a law professor, posted source code for encryption technology on a website for a law course.[15] He raised a First Amendment challenge to the regulations arguing that they were an unconstitutional prior restraint and content-based discrimination.[16] The 6th Circuit agreed that, in some cases, source code might be protected speech.[17] However, the court also recognized that the government may have a legitimate interest in regulating source code. It is difficult to draw a conclusion from these cases other than that the status of source code under the First Amendment remains to be decisively determined.

¶ 10 In light of these developments, companies or individuals who use encryption technology should be very careful spreading that technology. Even seemingly innocuous posting of source code on the Internet may violate the EAR and result in penalties. However, those interested in encryption technology should also keep abreast of current court decisions that may significantly impact their ability to spread the source code of encryption technology on the Internet.

Author: Matthew Crane

Footnotes

1. *Fact Sheet: How do I know if I need to get a license from the Department of Commerce?* at http://www.bxa.doc.gov/factsheets/facts1.htm(last visited August 13, 2001).

2. *Export Administration Regulations*, at http://w3.access.gpo.gov/bxa/fedreg/ear_fedreg.html(last visited August 13, 2001).

3. Fred M. Greguras & John Black, *Internet Export Compliance Issues for Software*, at http://www.batnet.com/oikoumene/software-inetxport.html(last visited August 12, 2001).

4. *Id*.

5. 34 Tex. Int'l L.J. 173, 182 (Spring 1999).

6. *Id*.

7. Fred M. Greguras & John Black, *Internet Export Compliance Issues for Software*, at http://www.batnet.com/oikoumene/software-inetxport.html(last visited August 12, 2001).

8. 15 C.F.R. 734.2(b)(9) (2001).

9. *Id*.

10. Karen Day, *The Experience of One Nation that has Implemented Intangible Transfer Controls*, at http://www.bxa.doc.gov/press/Archive2000/DayOxfordSpeech.html (September 27, 2000).

11. Fred M. Greguras & Roger M. Golden, *Access to U.S. Software and other U.S. Technology by Foreign Nationals*, at http://www.batnet.com/oikoumene/softwaccess_xprt.html(last visited August 13, 2001).

12. Karen Day, *The Experience of One Nation that has Implemented Intangible Transfer Controls*, at

http://www.bxa.doc.gov/press/Archive2000/DayOxfordSpeech.html(September 27, 2000).

13. *Commercial Encryption Export Controls: Regulations*, at http://www.bxa.doc.gov/Encryption/regs.htm(last visited August 13, 2001).

14. *Bernstein v. U.S. Dep't of Justice*, 176 F.3d 1132, 1140-41 (9th Cir. 1999), *reh'g granted en banc and opinion withdrawn*, 192 F.3d 1308 (9th Cir. 1999).

15. 114 Harv. L. Rev. 1813, 1814 (April 2001). The course website is http://samsara.law.cwru.edu/comp_law.

16. Id.

17. Junger v. Daley, 209 F.3d 481, 485 (6th Cir. 2001).