

IP ADVISOR

AN INFORMATIONAL NEWSLETTER FROM GOODWIN PROCTER LLP'S INTELLECTUAL PROPERTY GROUP

ARTICLE FROM APRIL
2008 ISSUE**SCRUTINY INTENSIFIES FOR ENCRYPTION EXPORTS***By Miguel Danielson*

As encryption has increasingly become part of modern technology architectures, so too has the burden of legal compliance for companies distributing such technology in the global marketplace. Nearly any software application that is capable of transmitting or receiving information over a network is likely to use some form of encryption, yet there is little awareness of the laws governing export of such encryption outside the United States. As regulators move to heighten the penalties associated with non-compliance, savvy companies in the technology sector are becoming keenly aware of encryption export issues and addressing them in a variety of contexts such as M&A, technology licensing and related business transactions. Any company that employs encryption in its products or supplies encryption-related technical data to others, therefore, should be well aware of the potential obligations incurred when it exports its products or technology outside the United States or contracts with third parties that desire to do so.

Generally, export laws, and more specifically encryption export laws, are not particularly user-friendly. The export of encryption technology is governed by the Export Administration Regulations (“EAR”), which cover the export of all non-military and commercial items outside the United States. The EAR are administered by the Bureau of Industry and Security (“BIS”), a division of the U.S. Department of Commerce. In addition to the EAR, there are other regulatory schemes that may be of relevance to the export of goods or technology pertaining to certain persons, entities or nations. For example, the Office of Foreign Assets Control of the U.S. Department of the Treasury controls exports to certain prohibited persons, entities and countries regardless of whether there are any EAR-related export controls involved.

Determining Encryption Export Obligations

The first step in determining an exporter’s obligations for an encryption item is to properly classify the item. Under the EAR, each controlled item is given a classification number that is used to determine an exporter’s obligations. The EAR contain an exhaustive list and description of all classification numbers, and any item that is not described by one of the delineated classifications falls into a “catch-all” classification for which there are no export obligations under the EAR (although other restrictions, discussed below, may still limit export to certain individuals, organizations or countries).

In many cases, exporters work with legal or export counsel to determine a product’s classification. Exporters may also, in addition, seek formal review from the BIS, which can provide classifications upon request. Once a classification number has been determined, the next step is to establish whether any exceptions to the general rule of required licensure for export exists. Over time, the BIS has significantly increased the number of instances in which encryption export may be undertaken without obtaining a

license – a process that can be both complex and time-consuming, and for which failure to obtain can have harsh ramifications, including fines, revocation of export rights and even criminal sanctions. Luckily, the relatively recent liberalization of the government’s policies on encryption export has meant that a good deal of encryption exports, particularly in the retail software and consumer technology markets, do not require a license to export to most jurisdictions. For example, a license may not be required for products that are marketed through traditional “mass market” retail channels, or for which the source code is publicly available, or if the applicable encryption is limited in its “strength” or ability to encrypt certain types of data. In determining whether any of the numerous exemptions apply, however, the specific facts of a particular case will need to be carefully examined by an expert in the relevant sections of the EAR, as export obligations are also dependent upon the identity of the end user of the product, the nature of the product used, and other relevant product facts.

It should also be noted that even where an exception to the licensing requirement does ultimately apply, an exporter is still likely to be obligated to take some action. For example, several of the available exemptions require that exporters file notifications or requests for abbreviated classification reviews with the BIS prior to export. The submission of such notifications or review requests can even be made by email in some situations, and in any event, most submissions to the BIS can also be made through an electronic filing system available over the Internet.

Skeletons in the Export Closet

In some cases, export obligations are identified only after the export has already been made. In such instances, companies are left with the quandary of addressing their past failings in contemplation of the continued desire to export within the confines of the regulatory requirements. Penalties for non-compliance range from monetary fines, denial of export rights to criminal prosecution. For companies that have discovered possible past violations of export regulations concerning encryption technology, the first step is always to seek appropriate counsel to determine whether a violation has in fact occurred. Once such a determination has been made, a company must then decide what approach to take, in light of the fact that there is a desire to both mitigate the risk of past violations and lay the groundwork for procedures that will prevent any additional future violations.

One technique that the existing regulations provides for is voluntary self-disclosure. While self-disclosure does not necessarily mitigate the sanctions related to an infraction under the EAR, it is influential to the BIS’s ultimate enforcement decisions. As with all decisions made by the BIS, however, the particular export facts are critical to any subsequent risk analysis as the BIS may choose to ignore the weight of a self-disclosure if aggravating factors are apparent. For this reason, anytime an exporter is in a position that may potentially lead to self-disclosure, appropriate counsel should be consulted for any attendant investigation, remediation or self-disclosure.

Additional Export Regulations

Beyond the EAR-specific controls on encryption export, the U.S. Government also carefully controls export of *all* goods to certain jurisdictions and to certain individuals or entities (and it is worth remembering that the exceptions under the EAR do not permit export to such jurisdictions without a license). For this reason, any company regularly exporting goods outside the United States should have in place a screening procedure

that detects exports to prohibited individuals, entities or jurisdictions, and is based on current lists of such parties.

Conclusion

The regulations governing export of encryption technology are complex and difficult to navigate, and the penalties for non-compliance can be harsh. Any company that exports software or technology containing encryption capabilities should take care to be in compliance with such regulations. Furthermore, companies that intend to regularly export controlled items outside the United States should institute procedures that will prevent their export to any prohibited individuals, entities or jurisdictions. By ensuring that any applicable export obligations are identified as early as possible, exporters can minimize both their potential risk and the cost of compliance.

If you would like further information about the topics covered in this newsletter, or any of the above publications or conferences, please contact Thomas J. Scott, Jr., chair of Goodwin Procter's Intellectual Property Group, at 202.346.4332 or tscott@goodwinprocter.com

Full access to articles on IP law prepared by Goodwin Procter is available at <http://www.goodwinprocter.com/Publications/FullIndexPublications.aspx>

This publication, which may be considered advertising under the ethical rules of certain jurisdictions, is provided with the understanding that it does not constitute the rendering of legal advice or other professional advice by Goodwin Procter LLP or its attorneys. Additionally, the foregoing discussion does not constitute tax advice. Any discussion of tax matters contained in this publication is not intended or written to be used, and cannot be used, for the purpose of avoiding penalties under the Internal Revenue Code or promoting, marketing or recommending to another party any transaction or matter.
© 2008 Goodwin Procter LLP. All rights reserved.