

ELECTRONIC EXPORT COMMERCE

The expansion of electronic commerce means that businesses will be able to market more easily their products and services to new foreign markets using the Internet to effect the sale. Where products are available in digital form (e.g., books, music, graphics, photographs, software, technical information, etc.) such products can be both sold and transferred to the end consumer directly through the Internet. In either case, Canadian businesses will increasingly have to consider the application of Canada's export control regimes to their activities.

Most business lawyers are aware that certain types of goods, such as those that contain encryption capabilities, may be subject to export controls. Many types of software programs, including browsers, word processing programs, database programs, and others incorporate encryption functions and are within the controls.

Overview of Canada's Export Control Regime

Export controls exist in order to fulfil Canada's obligations in bilateral and multilateral agreements. From 1950 to 1994, Canada was a member of the Coordinating Committee for Multilateral Strategic Export Controls (COCOM). On March 31, 1994, COCOM ceased to exist and the former COCOM members agreed to establish a new multilateral arrangement known as the "Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies."

In order to export goods that are (i) destined for a country on Canada's Area Control List (ACL), (ii) on Canada's Export Control List (ECL) or (iii) of U.S. origin, an exporter must first obtain a federal export permit from the Department of Foreign Affairs and International Trade (DFAIT). Regardless of the product, any goods going to a country on the ACL require a permit before they can be exported. Similarly, any nation that is embargoed by the United Nations may require additional approvals over and above any export permit.

Specific types of goods listed on the ECL require permits for export regardless of the destination. The ECL includes strategic goods and technologies such as those

that have military uses or have dual military and non-military uses. Cryptographic products are included on Canada's ECL.

Goods which originate in the United States are also controlled for re-export from Canada. In most cases, exporters can benefit from General Export Permit 12 (a sort of a blanket exemption that avoids the need to obtain individual export permits), which generally permits re-export of U.S. origin goods (subject to Canada's export control rules) except to certain designated countries.

The Wassenaar Arrangement obligates the imposition of controls on the export of hardware and software products which incorporate cryptographic capabilities. However, it provides some flexibility. While Canada already permits the export of cryptography products that are generally available to the public in Canada (under a "mass market" exemption), in a Notice to Exporters issued December 23, 1998, the federal government outlined proposed changes, expected to take effect before the end of 1999.

Some of these proposed changes would remove certain goods from control and therefore can be expected to have a positive effect on electronic commerce. For instance, controls are expected to be lifted from goods performing authentication and supporting digital signatures, where the cryptographic capability is not user-accessible, and is designed and limited to banking use or money transactions. It will likely also be removed from goods which employ a symmetric algorithm with a key length of 56 bits or less (in English, this means "weak encryption" that can be easily broken).

However, Canada, along with the other participating countries, also agreed to drastically narrow the availability of the current "mass market" exemption. The existing rules exempt software which is "generally available to the public" and "designed for installation by the user without further substantial support by the supplier." The new rules impose additional requirements: the cryptographic functionality must not be easily changeable by the user, and the product must not contain a symmetric algorithm employing a key length exceeding 64 bits (in other words, it must not support "strong encryption"). These restric-

page 2