Canadian Journal of Law and Technology

Volume 4 | Number 3 Article 5

8-1-2005

Cryptography Export Controls - Canada's Dichotomous Cryptography Policy

Paul Bates

CRYPTOGRAPHY EXPORT CONTROLS — CANADA'S DICHOTOMOUS CRYPTOGRAPHY POLICY

Paul Bates †

Introduction [1]

Cryptography makes electronic transactions more secure and reliable. Recognizing the importance of cryptography to e-commerce, the Canadian government adopted a digital cryptography policy in 1998. The policy provides for "digital freedom" for domestic cryptography by permitting Canadians to develop, import, and use for lawful purposes, any cryptographic products, without restrictions based upon the strength of the cryptography, the source of supply, the identity of the recipient, or the nature of the use.

Cryptography originated from military intelligence activities, principally in the Second World War. Advanced modern cryptography is vital to national defence undertakings. The military significance of cryptography is reflected in the classification of cryptography as a "Dual-Use Technology" in *The Wassenaar Arrangement on Export Controls for Conventional Weapons and Dual-Use Goods and Technologies* (WA).[2] The WA is an international accord between 33 nations, including Canada, dedicated to reducing the international distribution of dangerous goods and technologies. It was implemented in Canada through the *Export and Import Permits Act* (EIPA),[3] which was recently amended through the *Public Safety Act, 2002* (PSA)[4] in response to the September 11, 2001 terrorist attacks. Although the amendments have yet to come into force,[5] they will require a permit to transfer controlled cryptography out of Canada.

Canada's cryptographic policy, which promises domestic digital freedom, and the recent EIPA amendments, which fortify export controls, are inconsistent. This problem is amplified by the lack of borders in cyberspace. Export controls impose transaction costs on Canada's domestic cryptography industry and provide an incentive to locate cryptography research, development and production outside of Canada. For example, Israel has a significant cryptography development industry, and does not subscribe to the WA. The export controls may also impair expressive communications about cryptography through unconstitutional prior restraints on commercial and academic speech, contrary to the guarantee of freedom of expression in section 2 of the *Canadian Charter of Rights and Freedoms* (Charter).[6] The effort to erect strong legal barriers to trans-national distribution of cryptography has significant gaps because strong cryptography can be obtained and used within Canada without legal restrictions. This paper advocates that Canada should exercise its discretion under the WA to diminish, not fortify, the restrictions of the export control regime.

Export Controls

Wassenaar Arrangement

The WA received final approval by 33 co-founding countries[7] in July 1996, and was implemented in September 1996. It supplanted the *Coordinating Committee for Multilateral Export Controls* (COCOM) *Export Control Regime*, which ceased to exist on March 31, 1994.[8] COCOM was established in 1949 to control strategic goods and technology on the basis of informal agreement and consensus management. It maintained a secretariat in Paris, as well as permanent delegates.[9] At the end of the Cold War, the *COCOM Export Control Regime* recognized the need for a new arrangement to address risks to regional and international security from the spread of conventional weapons and dual-use goods and technologies.

The WA balances national security interests with commercial objectives through state objectives. The first purpose is to contribute to regional and international security and stability. This is achieved by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, and by preventing destabilizing accumulations of dangerous weapons. The second purpose is to complement and reinforce existing control regimes for weapons of mass destruction, without derogating from existing internationally recognized measures for this purpose. The third purpose is to enhance cooperation among the participating states to prevent the acquisition of armaments and sensitive dual-use goods and technologies, in areas or regions identified by the participating states to be of concern to them. The fourth purpose is a limiting prin-

†Barrister, Toronto, Ontario. The author gratefully acknowledges the research assistance of Cecilia Faeron and Tamara Lennox.

ciple juxtaposed against the security and stability objectives set out in purposes one through three: the participating states agreed not to impair or interfere with the rights of states to acquire legitimate means of self-defence, pursuant to Article 51 of the *Charter* of the United Nations. In addition, the participating states agreed not to impede lawful civil transactions. A fifth purpose was added at the seventh plenary session of December 2001, in reaction to the horrific events of September 11, 2001. The newest aim is to prevent terrorists from acquiring conventional arms and dual-use goods and technologies.

The WA is a voluntary protocol of member states. The WA states that, "[a]ll measures undertaken with respect to the Arrangement will be in accordance with national legislation and policies and will be implemented on the basis of national discretion".[10] The participating states are therefore free to determine the manner of implementation of the WA's objectives. They also reserve the right to transfer, or to deny transfer, of any item, subject to the WA's objectives.[11]

The WA contemplates that the participating states will exchange information on matters of concern, such as emerging trends in weapons programs, the accumulation of particular weapons systems, or other dangers according to a protocol derived from the categories of the UN Registrar of Conventional Arms. Any information exchanged under the WA is subject to confidentiality on the basis of privileged diplomatic communications.

The WA informs cryptography public policy formulation by the participating states. The basic feature of the WA is the control of the export of identified goods through export permits. The WA says nothing about intra-state transactions in goods; it applies to the export of goods and articles on the list of dual-use goods and technologies.

Implementation of the WA in Canada's Domestic Law

The WA was implemented in Canada by giving effect to executive powers conferred by the EIPA. The Governor in Council is empowered to create an Export Control List (ECL) under section 3 of the EIPA and an Area Control List (ACL) under section 4.[12] The identified purpose of the EIPA is "to implement an intergovernmental arrangement or commitment".[13]

The Permit Procedure

International Trade Canada, formerly the Department of Foreign Affairs and International Trade (DFAIT), considers the ECL to be a comprehensible statutory instrument for exporters who are presumed to be knowledgeable about the goods and articles they distribute. However, "[n]ovice users can find themselves swamped in so much information they lose sight of what they are looking for".[14] This is because the ECL is "a lengthy and very *technical* list of goods that require federal permits if they are exported".[15] International Trade Canada assists exporters by publishing *A Guide to Canada's Export Controls* (Guide),[16] which the ECL incorporates as law.[17] The Guide provides plain language answers to the following commonly asked questions:[18]

(A) Do I Need An Export Permit?

(B) Why Do Export Controls Exist?

(C) How Do I Obtain An Export Permit?

(D) Do I Need A Permit For Exports To The United States?

(E) Do I Need a Permit For The Export of U.S. Origin Goods or Technology?

(F) What Other Export Control Issues Should I Be Aware of?

(G) What Are The Export Permit Requirements For Forest Products?

(H) What Administrative Procedures Are Applicable In The Processing of Export Permits?

(I) What Supporting Documentation Is Required?

(J) What Does Customs Require And What Do I Do If My Goods Are Detained?

(K) What Is Canada's Legislative And Policy Basis For Export Controls?

(L) What Are Canada's Multilateral Commitments And How Do They Relate To The ECL?

(M) How Do I Use The ECL And Find Information In This Guide?

(N) What Goods Are Subject To Import Controls?

(O) What Are The Current Notices To Exporters?

(P) What Acronyms Are Used In This Guide?

International Trade Canada also publishes a Notice to Exporters,[19] which explains a number of expected changes to the export permit process for cryptographic goods and directs cryptography exporters to the appropriate permits.

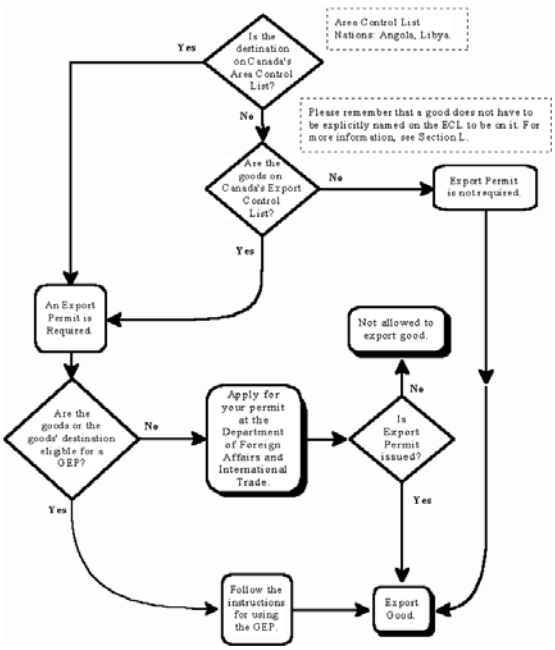
An exporter can apply for a General Export Permit (GEP) from International Trade Canada, by following the instructions set out in the GEP–Ext. 1042 "Application For Permit To Export Goods" Application Form.[20] A GEP enables an exporter to apply for a pre-authorization for imports and exports of certain eligible goods. However, qualification depends on whether the *goods or their destination* are in eligible classes; the GEP is referable to the character of goods and is not available for goods exported to states on the ACL or on the list of U.S. origin goods.

An individual export permit from International Trade Canada is required for U.S. origin goods and for the export of goods to states on the ACL. Exporters must consider the components of the goods, their origin and the permit requirements. International Trade Canada indicates that review and approval takes 10 working days and some goods require four to six weeks.[21] Customs Canada mandates that exporters who have obtained approval must record their approval number in Canada Customs B-13A documents when exporting goods.[22]

International Trade Canada does not reveal the criteria it applies in considering requests for export permits. One of the reasons for the lack of transparency is that International Trade Canada relies on discussions with other agencies and WA members in making its decisions, including the Canadian Security Intelligence Service, which may in turn consult the United States's national government security agencies.

The International Trade Canada Guide contains an index of ECL-controlled goods, but it is inconclusive, as it often refers to items using generic names or other terms, instead of common names. Exporters must therefore consider the numerous, complex descriptions and classifications of goods and technologies. International Trade Canada provides a flow chart of the decision-making involved in understanding the permit process:[23]

The decision process for obtaining a Federal Export Permit from Department of Foreign Affairs and International Trade[24]



Export permits for goods in group one (Category 1150: Information Security), which covers cryptography, are valid for two years, without extension.[25] The GEP is designed to minimize the administrative burden on exporters and to streamline licensing procedures; instead of submitting individual export permit applications, exporters can apply for general export permits that allow certain goods to be exported to eligible destinations. Examples of these GEPs are the *General Export Permit No. Ex. 18 — Portable Personal Computers and Associated Software*[26] and the *General Export Permit No. 39 — Mass Market Cryptographic Software.*[27]

The legal authority for the permit process is explained in the subsequent sections in the following sequence: the Area Control List, U.S. Origin Goods, and the Export Control List.

The Area Control List

The ACL controls goods based on their destination; it identifies the countries to which persons in Canada cannot export goods without a *special* permit.[28] The export of goods to these states is restricted, regardless of whether the goods are on any other control list. Myanmar (Burma) is currently the only country on this list.

U.S. Origin Goods — Item 5400 Group 5

Pursuant to Item 5400 Group 5 of the ECL, U.S. origin goods cannot be exported from Canada except by permit, to prevent the goods from being sent to countries that may use the goods inappropriately. Item 5400 defines U.S. origin goods as follows:

> *All* goods that *originate* in the United States, *unless* they are included elsewhere in this List, whether in bond or cleared by Canadian Customs, *other than* goods that have been further processed or manufactured outside the United States so as to result in a substantial change in value, form or use of the goods or in the production of new goods. (*All destinations other than the United States*)[29]

Irrespective of destination or nature, U.S. origin goods require an export permit.

The Export Control List

The ECL divides goods that require export permits into eight groups, based upon the goods' nature and component parts. Group 1 Item 1150 — Information Security[30] of the Dual-Use List[31] concerns cryptographic products. The restrictions and exemptions in this complex law must be reviewed with care.

The Restrictions of Items 1151–1155 of the ECL

Item 1150 of the Dual-Use List controls cryptographic products required for information security. It states that

> The control status of "information security"[32] equipment, "software"[33] systems, application specific "electronic assemblies,"[34] modules, integrated circuits, components or functions is determined in this Category even if they are components or "electronic assemblies" of other equipment.[35]

Item 1151 describes the following restricted systems, equipment and components:

> 1. Systems, equipment, application specific "electronic assemblies", modules or integrated circuits for "information security", as follows, and other specially designed components therefor: *N.B. For the control of global navigation satellite systems receiving equipment containing or employing decryption (i.e., GPS or GLONASS), see 1071.5.*
>
> (a) Designed or modified to use "cryptography" employing digital techniques performing any cryptographic function other than authentication or digital signature having any of the following:
>
> ***Technical Notes:***
>
> 1. *Authentication and digital signature functions include their associated key management function.*

2. *Authentication includes all aspects of access control where there is no encryption of files or text except as directly related to the protection of passwords, Personal Identification Numbers (PINs) or similar data to prevent unauthorized access.*

3. *"Cryptography" does not include "fixed" data compression or coding techniques.*

Note: *1151.1.a. includes equipment designed or modified to use "cryptography" employing analogue principles when implemented with digital techniques.*

1. A "symmetric algorithm" employing a key length in excess of 56 bits; *or*

2. An "asymmetric algorithm" where the security of the algorithm is based on any of the following:

(a) Factorization of integers in excess of 512 bits (e.g., RSA);

(b) Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g., Diffie-Hellman over Z/pZ); *or*

(c) Discrete logarithms in a group other than mentioned in 1151.1.a.2.b. in excess of 112 bits (e.g., Diffie-Hellman over an elliptic curve);

(b) Designed or modified to perform cryptanalytic functions;

(c) Deleted;

(d) Specially designed or modified to reduce the compromising emanations of information-bearing signals beyond what is necessary for health, safety or electromagnetic interference standards;

(e) Designed or modified to use cryptographic techniques to generate the spreading code for "spread spectrum" systems, including the hopping code for "frequency hopping" systems;

(f) Designed or modified to use cryptographic techniques to generate channelizing or scrambling codes for "timemodulated ultra-wideband" systems;

(g) Designed or modified to provide certified or certifiable "multilevel security" or user isolation at a level exceeding Class B2 of the Trusted Computer System Evaluation Criteria (TCSEC) or equivalent;

(h) Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion.[36]

Item 1152 refers to test, inspection and production equipment in terms very close to the WA:

1. Equipment specifically designed for

(a) The "development" of equipment or functions controlled by Category 1150, including measuring or test equipment;

(b) The "production" of equipment or functions controlled by Category 1150, including measuring, test, repair or production equipment.

(c) Measuring equipment specially designed to evaluate and validate the "information security" functions controlled by 1151 or 1154.[37]

Item 1153 is blank, as no restrictions have been categorized as materials.

Item 1154 refers to software as

1. "Software" specially designed or modified for the "development", "production" or "use" of equipment or "software" controlled by Category 1150.

2. "Software" specially designed or modified to support "technology" controlled by 1155.

3. Specific "software" as follows:

(a) "Software" having the characteristics or performing or simulating the functions of the equipment controlled by 1151 or 1152;

(b) "Software" to certify "software" controlled by 1154.3.a.[38]

Note that 1154 does not control

(a) "Software" required for the "use" of equipment excluded from control under the Note to 1151.

(b) "Software" providing any of the functions or equipment excluded from control under the Note to 1151.[39]

Item 1155 refers to technology as

1. "Technology" according to the General Technology Note for the "development", "production" or "use" of equipment or "software" controlled by Category 1150.[40]

Exemptions from Items 1150–1155 of the ECL

There are a number of exemptions from the description of controlled goods described in Items 1150–1155. Goods that fall within exemptions do not require export permits.

Item 1151 of the ECL exempts *specified technology* from the permit process of the EIPA, based on commercial application or use. This includes:

(a) "Personalized smart cards" where the cryptographic capability is restricted for use in equipment or systems excluded from control under entries b. to f. of this Note. If a "personalized smart card" has multiple functions, the control status of each function is assessed individually.

(b) Receiving equipment for radio broadcast, pay television or similar restricted audience broadcast of the consumer type, without digital encryption except that exclusively used for sending the billing or programme-related information back to the broadcast providers;

(c) Equipment where the cryptographic capability is not user-accessible and which is specially designed and limited to allow any of the following:

1. Execution of copy-protected software;

2. Access to any of the following:

(a) Copy-protected contents stored on read-only media; or

(b) Information stored in encrypted form on media (e.g., in connection with the protection of intellectual property rights) when the media is offered for sale in identical sets to the public; or

3. One-time copying of copyright protected audio/video data.

(d) Cryptographic equipment specially designed and limited for banking use or money transactions;

Technical Note:
"Money transactions" in 1151 Note d. includes the collection and settlement of fares or credit functions.

(e) Portable or mobile radiotelephones for civil use (e.g., for use with commercial civil cellular radiocommunications systems) that are not capable of end-to-end encryption;

(f) Cordless telephone equipment not capable of end-to-end encryption where the maximum effective range of unboosted cordless operation (i.e., a single, unrelayed hop between terminal and home base station) is less than 400 metres according to the manufacturer's specifications.[41]

The provisions of the General Technology Note (GTN) and the General Software Note (GSN) attenuate the force of the ECL as it relates to cryptographic products. These notes establish significant exemptions for *software in the public domain*, *mass market (retail) software*, *basic scientific research*, and the *minimum information necessary for a patent application*. The GTN states:

> The export of "technology" which is "required" for the "development", "production" or "use" of products controlled in the Dual-Use List is controlled according to the provisions in each Category. This "technology" remains under control even when applicable to any uncontrolled product.
>
> Controls do not apply to that "technology" which is the minimum necessary for the installation, operation, maintenance (checking) and repair of those products which are not controlled or whose export has been authorized.
>
> *N.B.: This does not release the repair "technology" controlled by Category in entries 1015.2.e. & 1015.2.f. and 1085.2.a. & 1085.2.b.*
>
> Controls do not apply to "technology", "in the public domain", to "basic scientific research"[42] or to the minimum necessary information for patent applications.[43]

The GSN provides that

> The Dual-Use List does not control "software" which is either
>
> 1. Generally available to the public by being:
>
> (a) Sold from stock at retail selling points, without restriction, by means of:
>
> 1. Over-the-counter transactions;
>
> 2. Mail order transactions; *or*
>
> 3. Telephone call transactions; *and*
>
> (b) Designed for installation by the user without further substantial support by the supplier; or
>
> ***N.B.***
> *Entry 1 of the General Software Note does not release "software" controlled by Category 1150.*
>
> 2. "In the public domain".[44]

Mass market software must be "in the public domain". The phrase "in the public domain" means technology or software that has been made available without restrictions upon its further dissemination. [*Copyright restrictions do not remove "technology" or "software" from being "in the public domain".*[45]] What is at any particular point in time "in the public domain" is a question of fact to be determined by International Trade Canada.

Interpretation of the EIPA Prohibition and Offence Provisions

The Nature of the Problem

The EIPA controls tangible objects based on national borders. This paper questions the efficacy of the EIPA with respect to the control of intangible software in borderless cyberspace.

The EIPA imposes export controls by prohibiting the export, or attempted export, of goods in contravention of the ECL and ACL, pursuant to section 13:

> No person shall *export* or attempt to export any *goods* included in an Export Control List or any goods to any country included in an Area Control List except under the authority of and in accordance with an export permit issued under this Act. [Emphasis added]

This section is reinforced by subsection 15(1), which is designed to capture any efforts at circumvention in third countries, as follows:

> Subject to subsection (2), except with the authority in writing of the Minister, no person shall *knowingly* do anything in Canada that causes or assists or is intended to cause or assist any *shipment*, *transhipment* or diversion of any *goods* included in an Export Control List to be made from Canada or any other place, to any country included in an Area Control List.
>
> (2) No person shall *knowingly* do anything in Canada that causes or assists or is intended to cause or assist any shipment, transhipment or diversion of any thing referred to in any of paragraphs 4.1(*a*) to (*c*), or any component or part designed exclusively for assembly into such a thing, that is included in an Export Control List, from Canada or any other place, to any country that is not included in an Automatic Firearms Country Control List. [Emphasis added]

The offence provision of the EIPA is found in subsection 19(1):

> 19(1) Every person who contravenes any provision of this Act or the regulations is guilty of
>
> (*a*) an offence punishable on summary conviction and is liable to a fine not exceeding twenty-five thousand dollars or to imprisonment for a term not exceeding twelve months or to both; or
>
> (*b*) an indictable offence and liable to a fine in an amount that is in the discretion of the court or to imprisonment for a term not exceeding ten years, or to both.

Interpretation of "Export"

"Export" is not defined in the EIPA, but is defined in *Black's Law Dictionary*[46] as follows:

> To carry or send abroad. To send, take, or carry an article of trade or commerce out of the country. To transport merchandise or goods from one country to another in the course of trade, to carry out or convey goods by sea. Transportation of goods from … to a foreign country.

The term "send" is defined in the *Black's Law Dictionary*[47] as a term used

> … in connection with any writing or notice means to deposit in the mail or deliver for transmission by any other usual means of communication with postage or cost of transmission provided for and properly addressed and in the case of an instrument to an address specified thereon or otherwise agreed, or if there be none, to any address reasonable under the circumstances. The receipt of any writing or notice within that time at which it would have arrived if properly sent has the effect of a proper sending.

The gravamen of an act of export is the transfer of something from inside Canada to outside Canada. It may not cover a situation where a person in Canada causes something to be transmitted from one location outside Canada to another location outside Canada. The EIPA would not prevent a Canadian cryptography vendor from receiving orders in Canada to ship cryptographic software from a server outside Canada to a recipient outside Canada. Consider the case of a Canadian cryptography supplier intending to make software available via the Internet. The EIPA requires the intent to transfer out of Canada. There are mechanisms available to zone commercial activity on the Internet, such as requirements for customers to certify their physical and digital locations. Suppose that a supplier decides to offer cryptography software from a Canadian server to customers who certify by reasonable means, such as digital certification, that their server is located in Canada. The Canadian supplier would not be required to inquire as to whether the receiving server in Canada is being used to transfer cryptography out of Canada. If the customer is located outside Canada and causes cryptographic software to be transmitted from the receiving server in Canada to outside Canada, the export act is committed by a person outside Canada and not the Canadian supplier, who would not know the customer's ultimate location.

The Interpretation of "Goods"

The use of the term "article" in section 3 of the EIPA reinforces the interpretation of "goods" as tangible objects. An article is defined as "a member of a class of things; *especially* an item of goods".[48] In *Black's Law Dictionary*, the definition of "goods"[49] is

> Goods — a term of variable content and meaning. It may include every species of personal property or it may be given a very restrictive meaning. Items of merchandise, supplies, raw materials, or finished goods. Sometimes the meaning of "goods" is extended to include all tangible items, as in the phrase "goods and services". All things (including specially manufacturing goods) which are movable at any time of identification to the contract for sale, other than the money in which the price is to be paid, investment securities and things in action. This also includes the unborn of animals and growing crops and other identified things attached to realty as fixtures. All things treated as moveable for the purpose of a contract of storage or transportation.

Cryptographic algorithms can be expressed in software posted on the Internet. Cryptography is intangible software. Can the definition of "goods" under the EIPA include intangible software? In *Regina v. Vanek, Ex parte Cross,*[50] the accused was charged under the EIPA with exporting bags of silver coins from Canada. The accused brought a motion to prohibit the hearing of the charges on the grounds that the term "goods" in the Export Control List did not include money, such as silver coins, and that it was *ultra vires* for the Order in Council to add silver coins to the list. The Court dismissed the application, holding that silver coins constituted "goods", which the Governor in Council properly added to the Export Control List. When not used as currency, the silver coins were goods.

Sections 13, 14 and 15 of the EIPA do not refer to "goods" and "articles" in isolation; these terms refer to the expansion in the ECL. The extensive definitions and detailed provisions of the ECL indicate a legislative intention to regulate cryptographic hardware and software. Category 1150 information security is defined in the Guide as

> All the means and functions ensuring the accessibility, confidentiality or integrity of information or communications, excluding the means and functions intended to safeguard against malfunctions. This includes "cryptography", cryptanalysis, protection against compromising emanations and computer security.[51]

Cryptography, on the other hand, is defined as

> The discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification or prevent its unauthorized use. "Cryptography" is limited to the transformation of information using one or more secret parameters (e.g., crypto variables) or associated key management.[52]

These definitions, to the extent that they cover abstract or intangible matters, are inconsistent with the natural and ordinary meaning of the word "goods" as referring to a tangible item. It is difficult to conceive of digital communication as goods. The Guide, which may evidence the legislative intention, suggests in several places that only tangible items are contemplated:

> Reminder: Canada Customs compares the *goods* described on the export permit and Customs Declaration form B-13A or equivalent export documentation with the contents of the shipment. Discrepancies in the documentation, including *goods* being exported without the required permit, could result in the export *being detained*, pending clarification, or in extreme cases, *seized*.[53]

These words imply that an element of physicality or tangibility is contemplated. It is unlikely that detention or seizure could refer to anything but tangible items.

It is questionable whether a string of zeros and ones, communicated using electric pulses, could be considered tangible.[54] In assessing a similar provision in the Australian export laws, solicitor Patrick Gunning[55] argued that Australian export controls must satisfy two conditions to apply to the supply of encryption software via the Internet.[56] First, software must come within the definition of "goods", and second, the transmission of data from a server in Australia to a person outside Australia

must constitute "exportation".[57] Gunning found support for his argument in Australia in the case of *Re: Michael Vickers,* which was similar to the *Vanek* case in Canada.[58] Mr. Vickers had $8,000 in cash and a credit balance of $15,000 in a bank account. Both were seized by customs officers pursuant to their authority to seize "goods" under the *Customs Act*. Morling J. held that the term "goods" as defined referred to tangible objects that are physically movable.[59] The credit balance in the bank account was not included in the term "goods".[60] Morling J. noted that it was "inappropriate to treat intangible things … as 'movables' for any purpose other than the conflict of laws".[61]

The case of *Toby Constructions Products Pty Ltd. v. Computer Bar (Sales) Pty Ltd.*[62] supports the argument that tangible qualities are contemplated in order for software to be considered goods. Rogers J. held that the sale of a computer system comprising both hardware and software constituted a sale of goods.[63] It was doubted whether the mere licensing of software (without the supply of any tangible products) also constituted a sale of goods. In the case of *ASX Operations Pty Ltd. v. Pont Data Australia Pty Ltd.*,[64] it was decided that, for the purposes of the *Trade Practices Act*, the term "goods" did not refer to encoded electrical signals. In *St. Albans City and District Council v. International Computers Ltd.*,[65] Sir Iain Glidewell made an important distinction between a software program and the physical medium on which it is encoded. The Court held that the physical medium, a computer disk, was considered a "good", but the program itself was not a "good".[66] The intellectual property involved in the software programme always remained with the author, and St. Albans merely received a licence to use the software.

It is arguable that cryptographic software in intangible form cannot be considered a "good" for the purpose of the EIPA. The abstract concepts of cryptography, and other information concerning algorithms cannot be considered goods for the purpose of the EIPA.

PSA: Amendments to the EIPA

The participating states of the WA have recognized the deficiencies in the EIPA restrictions on the "export" of "goods" and "articles"; amendments have therefore been introduced to control the "transfer" of "technology." These changes are included in Part 8 of the PSA and have yet to come into force. The long title of the EIPA will be changed to "[a]n Act respecting the export and transfer of goods and technology and the import of goods".[67] A new term, "technology," will be defined as follows:

> "technology" includes technical data, technical assistance and information necessary for the development, production or use of an article included in an Export Control List; [68]

A new term, "transfer", will be defined as follows:

> "transfer" means, in relation to technology, to dispose of it or disclose its contents in any manner from a place in Canada to a place outside Canada.[69]

The portion of section 3 of the EIPA before paragraph (*a*) will be replaced by the following:

> The Governor in Council may establish a list of goods and technology, to be called an Export Control List, including therein any article the export or transfer of which the Governor in Council deems it necessary to control for any of the following purposes:[70]

Section 4 will be replaced by the following:

> The Governor in Council may establish a list of countries, to be called an Area Control List, including therein any country to which the Governor in Council deems it necessary to control the export or transfer of any goods or technology.[71]

Technology as defined under the PSA includes cryptographic materials in both tangible and intangible media. Under the amendments, International Trade Canada can control and restrict all the technical means for developing, producing, or using any of the listed articles. In addition, "technical assistance and information" can include an individual's thoughts or memories with respect to the development, production, or use of the articles listed on the ECL. The use of the terms "dispose" and "disclose" expand the concept of "transfer" of technology; any exposure of the information, technical data, or technical assistance falls under this definition. International telephone conversations about restricted cryptographic products may be illegal. "[A]ny other place", as referred to in section 15 of EIPA, may restrict an academic in Canada from linking by video conference to an international conference attended by persons in a country on the Area Control List.[72]

Summary

In summary, WA amendments have been introduced to impose export restrictions. Strong cryptography cannot be exported or transferred out of Canada under the amendments, except by permit. However, it is problematic to apply controls that depend on national borders and the tangibility of objects to the transmission of intangible software and know-how on the Internet. There are significant gaps in the imposed barriers with mass market (retail) software, basic scientific research, the minimum information necessary for a patent application, and software in the public domain, notwithstanding copyright protection.

The EIPA does not prohibit persons in Canada from transferring cryptography from a source outside Canada to a customer outside Canada. In that case, there is no act of export. The EIPA may not prohibit persons in Canada from transferring cryptographic software from one server to another when both are located in Canada, again because there is no export. One or more of the following actions can avoid the restrictions of the WA:

- Domicile research operations outside Canada.
- Transfer cryptographic software from a server outside Canada, even if sales and marketing activities are located in Canada.

- Transfer cryptography products from a server in Canada to a recipient's server in Canada, relying on verified customer statements of location and intended use.
- Take the position that the EIPA does not apply to intangible cryptographic products.
- Place a cryptographic product in the public domain while maintaining copyright protection on the software.
- Produce mass market strong cryptography, since mass market software is not controlled.

Canada's Cryptography Policy

Canadian Law on Domestic Use and Development of Cryptography

There is a vibrant tension between cryptography export controls and Canada's policies concerning the importance of cryptography to the development of Canada's economy. In contrast to the export regime, domestic transactions involving cryptography are not subject to controls; there are no laws in Canada restricting the import and use of cryptography products of any strength. Market forces determine demand for, and the supply of, cryptography products for all applications, including stored data and real time communications. A supplier can distribute cryptography products of any strength to anyone in Canada, without considering the intended use of the customer, reporting the transaction to any public authority, or obtaining a licence to engage in the transaction. Canadians are free to access the supply of cryptography products from domestic or foreign suppliers. Cryptography products can be distributed by any means, whether in intangible form over the Internet or embedded in hardware or any other medium.

Canadian patent law grants intellectual property rights in cryptography products. Encryption software has been patented since the early 1980s. RSA Security has permitted free non-commercial use of its RSA algorithm with written permission for academic or university research purposes; the algorithm bears U.S. Patent Number 4405829 dated September 20, 1983.[73] On September 6, 2000, RSA Security waived its patent rights in the RSA algorithm and consented to the public dissemination of it. Similarly, U.S. Patent 3,962,539, which describes the Data Encryption Standard (DES), was assigned to IBM Corporation in 1976. IBM subsequently offered royalty-free licences conditional on adherence to the specifications of the standard, and the patent expired in 1993.[74] In addition to these, there are several important and well-established patents in cryptography, some of which have expired or been placed in the public domain. The patents in the category of strong encryption have been placed in Appendix 1 showing their date of issue and expiration for ease of reference.[75]

A patent is a species of intellectual property rights that depends upon the patent applicant making full disclosure in clear terms of the features of the patent. There is no territorial limitation on the availability of the information contained in an issued patent, so anyone can access patent information on file with the Canadian Patent Office from anywhere in the world for any purpose. This includes a patent on cryptography. As noted above, the EIPA explicitly permits the export from Canada of the minimum information necessary for a patent.

The Development of Canada's Cryptography Policy

Canada recognized the significance of e-commerce to the development of a robust and globally accessible economy, as well as the importance of participating in the global information infrastructure. E-commerce relies upon the transfer of, access to, and safe storage of digital information; the usefulness of cryptography in reducing threats to e-commerce is undisputable. The use of information technology has risen as increasingly powerful personal and networked computers communicate over converged systems on the universal Internet. The Internet supports both consumer and commercial activities, but also critical infrastructures such as energy, transportation, finance and communications. The nature, volume, and sensitivity of digitally enhanced information continue to expand, but this growth depends on the quality and dependability of cryptography.[76]

The growth and development of e-commerce depends upon the confidence of consumers and businesses in the safety and security of digital transactions. The poison of hackers and digital fraudsters threatens e-commerce. Cryptography is the antidote to this poison; it is both an art and a science for keeping secure data and real-time communications.[77] Cryptography has been described as the foundation of Internet commerce because it ensures security and confidentiality of electronic communications.[78] Cryptography serves the function of authentication, integrity, and non-repudiation. As summarized in an overview of the history of cryptography by the Canadian Security Establishment, "[s]oftware companies wish to protect their products against piracy, banks want to ensure secure transactions and almost everyone wishes to keep their personal information private."[79] The objects of information security are summarized in the *Handbook of Applied Cryptography*.[80]

Cryptography developed from a rarefied mathematical discipline in the domain of military intelligence strategists. There is now a major academic discipline in cryptography, exemplified in Canada by the Centre for

Applied Research in Cryptography at the University of Waterloo.[81] IBM,[82] Microsoft,[83] and PricewaterhouseCoopers[84] have organized corresponding international research and development activities.

Canada participated in the development of the 1997 Organisation for Economic Co-operation and Development (OECD) Guidelines on Cryptography Policy. The OECD Guidelines posited that national and global information infrastructures were developing rapidly to provide a seamless network for worldwide communications. To make this possible, users of information technology must have trust in the security of information and communications. The Guidelines consisted of a set of eight principles to be weighed by nations in developing their national cryptography policy frameworks.[85] The recommendations can be summarized as follows:

1. Cryptography should be used to foster confidence in information and communications infrastructures, and to protect data security and privacy.
2. Users should have the right to choose any cryptographic method, subject to applicable laws.
3. Government controls on cryptographic methods should be no more than are essential to the discharge of governmental responsibilities.
4. Market forces should dictate the development in cryptographic methods.
5. Technical standards, criteria, and protocols for cryptographic methods should be developed and promulgated at the national and international level.
6. The fundamental rights of individuals to privacy, including secrecy of communications and protections of personal data, should be respected in national cryptography policies, in the implementation and the use of cryptographic methods.
7. In the case of encrypted data, it was contemplated that national cryptography polices may allow lawful access to cryptographic keys or plaintext.
8. Civil liability regimes should be applicable to cryptographic service providers or parties obtaining access to cryptographic keys or plaintext, by means of contract or otherwise. It was particularly recommended that cryptography policies should not be implemented so as to create unjustified obstacles to trade.

The OECD Guidelines reflected that globalization is an integral element of business. "In a global trading environment, the full advantages of electronic commerce can only be achieved through a transition to open networks."[86] However, open networks are susceptible to information piracy:

> In the world of open networks and in an environment which is increasingly characterized by uncertainty and global economic competition, strong encryption enables corporations to protect themselves from competitive intelligence-gathering and criminal threats, and to protect sensitive information and communications.[87]

Cryptography is necessary in a borderless world to enhance the creation of "virtual organizations" and forge "strategic partnerships" in cyberspace.

In February 1998, the Government of Canada produced a White Paper entitled "Cryptography Policy Framework For Electronic Commerce: Building Canada's Information Economy and Society" under the auspices of the Task Force of Electronic Commerce mandated by Industry Canada. Canada's cryptographic policy provided for the development of a public key infrastructure (PKI) that "will interface with private sector and institutional PKIs adhering to similar levels of privacy, integrity and security standards, in order to provide the easy and seamless secure electronic transactions demanded by Canadians".[88] Canada has earned a reputation as a world leader in telecommunications and software sectors, with strength in cryptography products.

There is much to be said for the degree of consultation undertaken by the government of Canada in respect of cryptography policy. The stakeholders are easily ascertained. There are the diverse police forces and security agencies, which consider that cryptography is a threat to law enforcement activities because it facilitates concealment and execution of criminal activity. There is the domestic cryptography industry, with a gross direct production of about $300–$350M in annual volume, almost 90% of which is exported.[89] This industry employs approximately 1300 persons, about 5% of the Canadian workforce in information and telecommunications industries.[90] This industry has been demanding a review of Canada's adherence to WA export controls, contending that these controls inhibit the competitive development of the domestic industry.

A consultation process regarding export controls occurred in 1998. At that time, Industry Canada published "A Cryptography Policy Framework for Electronic Commerce", which called for responses from participants to be presented over the ensuing months. In total, over 200 responses were received,[91] with two competing themes regarding export controls. Canada was being placed at a competitive disadvantage by the current application of export controls, and it was necessary to maintain adherence to the WA in concert with the international community. Only 7% of respondents favoured maintaining the *status quo* or extending export controls; there was a clear overall preference for the elimination of export controls. Some noted that the WA restrictions were being interpreted in various ways by other states, notably more stringently by the United States, while European states such as Germany, Switzerland, and Ireland did not follow the WA protocols. The domestic cryptography industry strongly submitted that Canada should take maximum advantage of the flexibility in

application of the WA provisions contemplated by the terms of that arrangement.[92]

The result of the consultation process was an adjustment in the implementation of export controls, which Minister Manley announced in a speech on October 1, 1998:

> Fourth, we will continue to implement cryptography export controls within our commitments to the Wassenaar Arrangement; however, we will ensure that Canadian cryptography manufacturers face a level playing field — our controls will take into account the practices of other countries so that Canadian manufactures will not be at a competitive disadvantage.
>
> Fifth, we will streamline the export permit process and make it more transparent. For many products, users or destinations, after a "one time review" of the product, general or multi-destination, multiuser permits will be issued. Our intention is to simplify and speed up decision making, and significantly reduce the "regulatory drag" on exporters. We do not want them to be late to market.[93]

These policies were implemented by a Notice to Exporters under the EIPA, explaining intended changes to the permit process for "Export Controls on Cryptographic Goods".[94] The purpose of the Notice to Exporters was stated to be to inform the exporting community of

> (a) proposed changes to Canada's export controls on cryptographic goods as a result of recent changes to the Wassenaar Arrangement Lists of controlled goods and technology; and
>
> (b) the procedures that have been implemented to streamline the export permit process for cryptographic goods to make the process more transparent.[95]

The intent of the proposed amendments was to streamline the export process, "to better position Canadian exporters to increase their sales and share in global markets while being mindful of security interests".[96] The liberalizations contemplated by the Notice to Exporters were in accordance with the actions of the participating states of the WA as described in its annual protocols. First, goods were to be removed from controls if they performed certain functions of particular assistance to e-commerce. These included authentication, digital signature, PINs, key lengths of 56 bits or less, asymmetric algorithms within specified parameters defined by industry standards (RSA, Diffie-Hellman, etc.), consumer broadcast signals, non-user-accessible encryption technologies used for securing software and copyright-protected media, goods designed for banking and money transactions, and limited wireless communications equipment.[97] In addition, reporting requirements were to be removed. The exemption from export controls for goods in the public domain was to be maintained.[98]

The Notice to Exporters articulated Canada's commitment to encourage the widespread use of strong encryption and the growth of export markets for Canadian technologies.[99] Subject to these differences, Canada continues to adhere to the WA.

A test of the efficacy of these changes was undertaken by AEPOS Technologies Corporation in the "Exploratory Review", which was completed in 2000, but was not released to the public. A "Report to Consultation Participants" was released on March 7, 2001.[100] The sensitive subject of export controls was presented as follows:

> The issue of export controls *per se* did not appear in the data collection template nor was it our intention to raise the subject, but many companies expressed concern over the way export controls are being applied and administered by the federal government. Usually the issue was raised in response to one or more of the following questions:
>
> *Are there any factors that make it difficult for the company to conduct its development, production or research activities in Canada?*
>
> *Are there factors that might cause the company to move operations/research outside the country? If so, what are they?*
>
> *Are there factors that would encourage the company to do more work in Canada or repatriate some of the work currently done abroad? And*
>
> *Are there obstacles to growth in Canada?*
>
> Three areas of concern were mentioned repeatedly: the fact that mass market/retail crypto is treated differently by the U.S. and Canada when processing export applications (i.e., the U.S. is more liberal in applying Wassenaar rules); the excessive time taken to respond to companies when they apply for an export permit or try to get direction or guidance; and the requirement for end-user statements which, it is claimed, potentially create unlimited liability.
>
> The concerns over export issues were reflected in detail in the body of the report.[101]

The study indicated that it is widely regarded as very important for Canada to maintain a strong and independent cryptographic capability in the face of increasing internationalization of the industry. Canada's strengths in cryptography are widely recognized and respected, and loss or diminution of such expertise would adversely affect Canada's ability to play a major role in helping develop complex applications.

A revision of this consultation process was undertaken during the legislature's process to amend the EIPA, leading to a re-statement of the reservations of the domestic industry with regard to the imposition and application of export controls:

> None of the companies has considered in detail the possible effects of the new legislation (Bills C36, 42 [changed to Bill C-[7]] & 44) and companies are not particularly concerned as long as cryptography export regulations continue to be administered as they are being administered now. However, if the new law were to be applied in a way that makes the export of cryptography (or any other sort of technology or intellectual property) more difficult, industry would not be happy.[102]

The domestic cryptography industry is aware of the lack of uniformity and consistency in implementation by WA Participating States and others. The Global Internet Liberty Campaign published an international survey of encryption policies.[103] The survey was conducted by the

Electronic Privacy Information Centre (EPIC) and was a follow-up to submissions to the OECD in connection with the OECD's development of cryptography policy in 1996. It revealed the inconsistency amongst nations with regard to policies and laws on this area. It also demonstrated the controversy over and lack of uniformity in the implementation of WA-style export controls within Canada and elsewhere. This point is expansively demonstrated in the research embodied in Grabow's "Changes in Cryptographic Export-Import Rules".[104]

Expressive Cryptography

The term "expressive cryptography" refers to the concept that cryptography consists of more than bits and bytes; it includes a field of science in which mathematicians strive to develop advanced algorithms, create codes, break codes, and design systems to generate these codes. These activities may take place at renowned academic institutions populated by scholars, and in industry carrying on business in the mainstream economy. These activities may take place in the minds and purposes of cyber-criminals. How do the WA export controls affect these diverse activities? Specifically, can the export controls be applied to restrict academic and commercial communication of cryptography concepts and products? One consideration that should inform the EIPA amendments is whether they infringe upon freedoms guaranteed under the Charter, specifically paragraph 2(*b*) which generates freedom of expression.

The Supreme Court in *Irwin Toy v. Quebec (Attorney General)*[105] defined constitutionally protected expression as that which communicates thoughts, ideas or meaning. Commercial expression is protected by paragraph 2(*b*). This holding was reiterated in *RJR-Macdonald Inc. v. Canada (Attorney General)*,[106], and in *R. v Guignard*.[107] According to Prof. Hogg, "so long as the [criminal] activity is communicative, and falls short of the direct infliction of violence, it is protected by s. 2(*b*)."[108]

The same issues arose in *Bernstein v. United States Department of Justice*.[109] A mathematics academic named Bernstein asked the Office of Defense Trade Controls whether an export permit was required to publish a cryptographic algorithm called "Snuffle", a computer source code, and an English description of the algorithm. After being advised that all aspects of his research were subject to export licensing requirements, Bernstein sought a declaratory judgment preventing the Department of State from enforcing export controls in relation to his travel to an international conference of cryptographers. The California District Court ruled that the licensing requirement for the export of cryptographic software was an unconstitutional prior restraint of protected speech. In addition, the Court deemed the cryptographic computer source code protected speech under the First Amendment and the permit regime unconstitutional prior restraint.

The U.S. case of *DVD Copy Control Association v. Bunner*[110] concerned an appeal against a prior restraint order, which prohibited the defendants from republishing decryption software on their web sites. This software decrypted the encryption code limiting access to DVD movies. The issue before the Court was whether the First Amendment to the United States Constitution protected the publication of cryptographic information as an exercise of free speech. The California Court of Appeal concluded that computer source code[111] contained communicative elements and was constitutionally protected speech:

> The fact that a medium of expression has a functional capacity should not preclude constitutional protection … [C]omputer source code, though unintelligible to many, is the preferred method of communication among computer programmers. Because computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment. (*Junger v. Daley* (6th Cir. 2000) 209 F.3d 481, 484-485).[112]

The U.S. Second Circuit of Court of Appeals in *Universal City Studios Inc. et al. v. Corley*[113] also held that computer code is constitutionally protected speech because it is a medium for the communication of human thoughts or ideas.[114]

In Canada, computer source code, a human-readable language of expressing thoughts and commands on the operation of computers, would be considered a form of expression eligible for constitutional protection. Canadian law protects all media for expressing meaning, including words and non-verbal language. The requirement of an export control permit is a prior restraint or limit on freedom of expression. "[A] prior restraint is a law that prohibits the publication of particular material either absolutely or under a requirement of prior approval by a censor."[115] Cryptographic expression that is never published cannot contribute in any way to the marketplace of ideas, to personal fulfillment, or to actualization.

As the export controls would require a permit to transmit across Canadian borders restricted cryptography, the question is whether EIPA restrictions on expressive forms of cryptography can survive a section 1 Charter analysis. *R. v. Oakes*[116] outlined four criteria that a law must meet to impose reasonable and justifiable limits on rights in a "free and democratic society":

1. Sufficiently important objective: The law must pursue an objective that is sufficiently important to justify limiting a *Charter* right.
2. Rational connection: The law must be rationally connected to the objective.
3. Least drastic means: The law must impair the right no more than is necessary to accomplish the objective.
4. Proportionate effect: The law must not have a disproportionately severe effect on the persons to whom it applies.[117]

Part 2 of the *Oakes* test focuses on a rational connection between the objective of the law and the measures enacted by the law. Strong encryption theory is taught at universities and published in numerous books available worldwide and on the Internet. There is nothing in the PSA restricting foreigners from coming to Canada to participate in cryptography conferences. The objective of the EIPA in implementing the WA is to restrict the distribution of strong cryptography. The ECL suffers from inconsistency, as it prohibits the export of strong cryptography, unless it is in the public domain, but there is no prohibition against putting strong cryptography in the public domain. This means that a Canadian academic intending to disseminate a treatise containing information on strong cryptography must publish his or her paper before traveling abroad to a conference to present it. The inconsistency in the ECL is accentuated by the absence of legal controls of any kind on the domestic distribution of strong cryptography. If expressive versions of strong cryptography can be disseminated in Canada without restriction and placed in the public domain worldwide, why cannot they be transmitted to an identified recipient out of Canada without a permit? The experience of the U.S. with its export controls[118] indicates that the gaps in export controls may make them ineffective. According to Kerben, the U.S. government's asserted interest in national security failed to account for the fact that the number of encryption products in foreign countries had steadily risen to the point that foreign corporations were supplying the American market with encryption products.[119] Recognizing this, the U.S took steps in 2000 to scale down its export restrictions on powerful encryption technology, in an effort to match the European Union's liberalization of rules governing the export of encryption products.[120]

The EIPA amendments are constitutionally suspect, to the extent that they restrict the dissemination of expressive forms of cryptography. There is a continuum of communication in cryptography, from politically motivated presentations of strong cryptography, such as that by digital anarchists, to source code that may be exchanged between vendors and consumers of software products. The closer the facts are to academic and political expression about cryptography, the greater the likelihood that the EIPA amendments and the ECL restrictions will be declared unconstitutional in their design, or their application to particular fact situations. Limitations on publication of cryptography cannot be justified when that cryptography material is available to foreigners in Canada. It is difficult to imagine that the export of cryptographic technology originating in Canada would "generate a national security threat when equivalent and even superior technology is already available abroad".[121]

It is recognized that public security concerns constitute an important governmental objective for the purposes of the *Oakes* test, part 1.[122] The court will defer to legislative measures to address concerns relating to public safety.[123] But the means employed to address these concerns will be subject to judicial scrutiny in which core constitutional values, such as freedom of expression, are at stake. The gaps in export controls, and the dichotomy in domestic freedom to discriminate against all cryptography, create a significant risk that legislative controls on expressive cryptography will be found to contravene the Charter.

Conclusions

The government of Canada has taken major steps forward in the adoption of a cryptography policy that is dedicated to the development of Canada's domestic cryptography industry. The policy is part of the basic objective to make Canada a world leader in e-commerce, and cannot be accomplished without the security provided by effective cryptography and other means.

There is an inconsistency between the policy of domestic digital freedom in cryptography and the restrictions imposed by export controls. A policy choice must be made: should export controls be further relaxed within the parameters of the WA? There are serious defects in the WA, particularly as applied to the distribution of intangible cryptography on the Internet. There is no evidence that export controls are an effective method of preventing the distribution of strong cryptography. There is no empirical evidence that strong cryptography does not already exist in the states identified on the ACL. The ECL has significant loopholes — mass market and public domain cryptographic products are not controlled, and cryptographic algorithms and information can be found on the Internet.

The current EIPA provisions do not apply to Internet distribution of intangible cryptography. The proposed amendments are unlikely to withstand a constitutional challenge, and can easily be circumvented by simple methods, such as requiring customers to provide a domestic Internet address for transmission of cryptographic software.

The WA text makes it clear that participating states are entitled to implement the WA in the manner they deem appropriate under their national policies and laws. The actions of any one participating state, such as the control of cryptographic technology, do not obligate other states to adhere to the same public policy. Canada is free to adopt and implement a made-in-Canada policy for the export of cryptographic goods.

Canada should exercise its discretion under the WA to remove *ex ante* export controls, in favour of a simple registration system that requires exporters to notify International Trade Canada of transactions involving the supply or sale of cryptographic products to customers outside Canada. There should be no requirement to obtain a permit in advance; domestic producers should not be vulnerable to the uncertainty of whether an

export permit will be granted, and when. The timing and pace of cryptography transactions should be determined entirely by commercial considerations, not regulatory efficiencies. Reporting cryptography transactions should be sufficient to enable Canada to participate in the reporting and consultation process contemplated by the WA. In this way, Canada's cryptography policy will become more consistent with the objectives of making Canada a world leader in e-commerce.

APPENDIX 1

Important Patents in Cryptography[124]

PATENT	INVENTOR	PATENT ORIGIN AND #	DATE FILED	DATE ISSUED	ASSIGNEE	PUBLIC DOMAIN	EXPIRED
DES[125]	Ehrsam et al.	US #3, 962, 539	February 24, 1975	June 8, 1976	IBM	Yes	Yes
Diffie-Hellman[126]	Hellman, Diffie and Merkle	U.S. Patent: 4,200,770	September 6, 1977	April 29, 1980	Stanford University	Yes	Yes
Public-key cryptosystems[127]	Hellman and Merkle	U.S. Patent: 4,218,582	October 6, 1977	August 19, 1980	Stanford University	Yes	Yes
RSA[128]	Rivest, Shamir, Adleman	U. S. Patent 4, 405, 829	December 14, 1977	September 20, 1983	MIT		
Fiat-Shamir identification[129]	Shamir and Fiat	U.S. Patent: 4,748,668	July 9, 1986	May 31, 1988	Yeda Research and Development (Israel)		
Control vectors[130]	Matyas, Meyer, and Brachtl	U.S. Patent: 4,850,017	May 29, 1987	July 18, 1989	IBM		
GQ identification[131]	Guillou and Quisquater	U.S. Patent: 5,140,634	October 9, 1991	August 18, 1992	U.S. Phillips Corporation		
DSA[132]	Kravitz	U.S. Patent: 5,231,668	July 26, 1991	July 27, 1993	United States of America		
Fair cryptosystems[133]	Micali	U.S. Patent: 5,315,658	April 19, 1993	May 24, 1994	none		

Notes:

[1] Best efforts were undertaken to represent the law and any references as of August 15, 2005.

[2] "Welcome to the Wassenaar Arrangement", online: The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies: http://www.wassenaar.org/welcomepage.html (date accessed: 30 May, 2005) [*WA*].

[3] R.S.C. 1985, c. E-19 [*EIPA*].

[4] Bill C-7, *An Act to amend certain Acts of Canada, and to enact measures for implementing the Biological and Toxin Weapons Convention, in order to enhance public safety*, 3rd Sess, 37th Parl., 2004 (received Royal Assent on May 6, 2004). Online: Library of Parliament http://www.parl.gc.ca/LEGISINFO/ index.asp?Lang=E&Chamber=N&StartList=A&EndList=Z&Session=12&Type=0&Scope=I&query=4097&List=toc-1 (date accessed: 30 May, 2005).

[5] The EIPA amendments in the PSA will come into force on a day or days to be fixed by order of the Governor in Council.

[6] *Canadian Charter of Rights and Freedoms*, Part 1 of the *Constitution Act, 1982*, being Schedule B to the *Canada Act*, 1982 (U.K), 1992, c. 11 [*Charter*].

[7] Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russian Federation, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom and the United States.

[8] On November 16, 1993, representatives of the 17 COCOM member states agreed to terminate COCOM's operations and activities.

[9] See U.S. Department of State, "COCOM — An End and A Beginning", online: U.S. Department of State, Defense Trade News http://cryptome.quintessenz.org/mirror/dtn0494.htm as cited in note 50 in N. Ellsmore, "Cryptology: Law Enforcement & National Security vs. Privacy, Security & The Future of Commerce", online: <http://cryptome.quintessenz.org/mirror/crypto97-ne.htm> (date accessed: 15 August, 2005) [*Ellsmore*] at 56.

[10] "Initial Elements," online: The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies http://www.wassenaar.org/docs/IE96.html (date accessed: 30 May, 2005).

[11] It is a general principle of Canadian constitutional law that treaties must be specifically incorporated into domestic law to have effect. See *Ahani v. Canada (Attorney General)* (2002), 58 O.R. (3d) 107 (C.A.) at 118. Any implementation in domestic law must be in accordance with domestic constitutional principles.

[12] Myanmar (Burma) is currently on Canada's Area Control List. The Area Control List will be discussed *infra*.

[13] *EIPA*, *supra* note 3 at paragraph 3(*d*).

[14] "Export Control List — ECL Introduction,", online: http://www.dfait-maeci.gc.ca/trade/eicb/menu-en.asp (date accessed: 30 May, 2005) [*ECL*].

[15] "Military and Technology Export Control List,", online: http://www.dfait-maeci.gc.ca/trade/eicb/military/intro-en.sap?#m (date accessed: 15 August, 2005) [emphasis added].

[16] "Military, Technology and Miscellaneous Exports, Export Control List,", online: International Trade Canada http://www.dfait-maeci.gc.ca/trade/eicb/military/content-en.asp (date accessed: 30 May, 2005) [*The Guide*].

[17] International Trade Canada, "Notice to Exporters" (December 1998) at section 3, online: International Trade Canada http://www.dfait-maeci.gc.ca/trade/eicb/notices/ser113-en.asp (date accessed: 30 May, 2005) [*Notice to Exporters*].

[18] *The Guide*, *supra* note 16.

[19] *Notice to Exporters*, *supra* note 17.

[20] *The Guide*, *supra* note 16.

[21] *Ibid.*, under heading "C: How do I Obtain a Permit?" at para. 4.

[22] *Ibid.*, at para. 3.

[23] International Trade Canada,"Military Technology and Miscellaneous Exports, Export Control List,", online: http://www.dfait-maeci.gc.ca/trade/eicb/general/general-en.asp (date accessed: 24 February, 2004).

[24] *The Guide*, *supra* note 16.

[25] *The Guide*, *supra* note 16, under heading "C: How Do I Get An Export Permit?" at para. 4.

[26] *General Export Permit No. Ex. 18 — Portable Personal Computers and Associated Software*, [SI/89-121]:

> 2. Subject to section 3, any person may, under the authority of this Permit, export from Canada for a period not exceeding three months, portable personal computers and associated software designed for use in those portable personal computers, on condition that
>
> (*a*) no transfer of technology takes place as a result of the exportation of the portable personal computers and their associated software; and
>
> (*b*) the portable personal computers and their associated software are used only by the exporter and only for business or education purposes.
>
> 3. This Permit does not authorize the exportation of goods described in section 2 to any country listed on the *Area Control List*. SI/90-94, s. 1.

[27] *General Export Permit No. 39 — Mass Market Cryptographic Software*, [SOR/99-238]:

> 2. Subject to sections 3, 4, and 5, any resident of Canada may, under the authority of and in accordance with this Permit, export mass market cryptographic software from Canada.
>
> 3. This Permit does not authorize the exportation of mass market cryptographic software to any country listed in the *Area Control List* or to any of the following countries:
>
> (*a*) Democratic People's Republic of Korea (North Korea);
>
> (*b*) Iran; and
>
> (*c*) Iraq.
>
> 4. It is a condition of this Permit that the exporter
>
> (*a*) keep at the exporter's place of business or residence the documents in respect of each export made under this Permit for a period of six years after the date of the export; and
>
> (*b*) on request, make the documents referred to in paragraph (a) available to an officer of the Export Controls Division.
>
> 5. On request, the exporter must provide details of the mass market cryptographic software to the Export Controls Division.

[28] *Area Control List*, SOR/89-201, s. 2 *(f)*: Myanmar is currently the only country listed on the ACL.

[29] *The Guide*, *supra* note 16, under heading "E: United States Origin Goods". This restriction applies to re-exporting to all destinations except the U.S.

See *General Export Permit No. 12 — United States Origin Goods*, sections 1 and 2 [SOR/97-107] referring to items 5400–5401 of Group 5 of the Schedule to the *Export Control List*:

> 1. Subject to section 2, any person may, under the authority of this Permit, export from Canada any goods of United States origin as described in item 5400 of Group 5 of the Schedule to the *Export Control List*.
>
> 2. This Permit does not authorize the exportation of goods described in section 1 to any country listed in the *Area Control List* or to any of the following countries:
>
> (*a*) Cuba;
>
> (*b*) Democratic People's Republic of Korea;
>
> (*c*) Iran; and
>
> (*d*) Libya.
>
> SOR/99-203, s. 1.

[30] This corresponds with Category 5 Part 2 of the Wassenaar Lists. See *WA*, *supra* note 2.

[31] "Dual-Use" items are industrial products with a civilian/military or nuclear/non-nuclear use.

[32] *Ibid.*, Defined in *The Guide*, *supra* note 16 as, "[a]ll the means and functions ensuring the accessibility, confidentiality or integrity of information or communications, excluding the means and functions intended to safeguard against malfunctions. This includes 'cryptography', cryptanalysis, protection against compromising emanations and computer security. **N. B.:** 'Cryptanalysis' is the analysis of a cryptographic system or its inputs and outputs to derive confidential variables or sensitive data, including clear text. (ISO 7498–2–1998 (E), paragraph 3. 3. 18.)". "Definitions of Terms Used in Groups 1 and 2,", online: International Trade Canada http://www.dfait-maeci.gc.ca/trade/eicb/military/gr1-2-en.asp [*Definitions*] (date accessed: 30 May, 2005).

[33] *Ibid.*, Defined in *The Guide* as "[a] collection of one or more 'programmes' or 'microprogrammes' fixed in any tangible medium of expression". Programme is defined as "[a] sequence of instructions to carry out a process in, or convertible into, a form executable by an electronic computer". The term "Micro-programme" is defined as "[a] sequence of elementary instructions maintained in a special storage, the execution of which is initiated by the introduction of its reference instruction register."

[34] *Ibid.*, Defined in *The Guide* as, "[a] number of electronic components (i.e., 'circuit elements', 'discrete components', integrated circuits, etc.) connected together to perform (a) specific function(s), replaceable as an entity and normally capable of being disassembled". "Circuit element" is defined as "[a] single active or passive functional part of an electronic circuit, such as one diode, one transistor, one resistor, one capacitor, etc." "Discrete component" is defined as "[a] separately packaged 'circuit element' with its own external connections". (*Definitions*, *supra* note 32).

[35] *The Guide*, *supra* note 16, under heading "Category 1150: Information Security", online: International Trade Canada http://www.dfait-maeci.gc.ca/trade/eicb/military/gr1150-en.asp?#category1150 (date accessed: 30 May, 2005).

[36] *The Guide*, *supra* note 16, under heading: "Category 1150", online: International Trade Canada http://www.dfait-maeci.gc.ca/trade/eicb/military/gr1150-en.asp?#category1150 (date accessed: 30 May, 2005).

[37] *Ibid.*

[38] *Ibid.*

[39] *Ibid.*

[40] *Ibid.*

[41] *Ibid.*

[42] *Definitions*, *supra* note 32. Defined in *The Guide*, *supra* note 16 as "[e]xperimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective".

[43] *The Guide*, *supra* note 16, under heading: "Group 1 — Dual-Use List", online: International Trade Canada http://www.dfait-maeci.gc.ca/trade/eicb/military/gr1-en.asp?#generaltechnologynotesoftwarenote (date accessed: 30, May, 2005) [emphasis added].

[44] *Ibid.*

[45] *Definitions*, *supra* note 32.

[46] *Black's Law Dictionary*, 7th ed., *s. v.* "export" [*Black's*].

[47] *Ibid.*, *s.v.* "send".

[48] "Merriam-Webster Online Dictionary", online: Merriam-Webster OnLine http://www.merriamwebster.com [emphasis in original].

[49] *Black's*, *supra* note 45, *s. v.* "goods".

[50] [1969] 2 O.R. 724 (H.C.J.) [*Vanek*].

[51] *Definitions*, *supra* note 32.

[52] *Ibid.*

[53] *The Guide*, *supra* note 16, under heading: "What Does Customs Require and What Do I Do if My Goods Are Detained or Seized?", online: International Trade Canada http://www.dfait-maeci.gc.ca/trade/eicb/military/intro-en.asp?#j (date accessed: 30 May, 2005). Note that *The Guide* was recently updated to refer to goods and technology (date accessed: 15 August, 2005):

> *Reminder: CCRA compares the goods and technology described on the export permit and the Customs Export Declaration form B-13A or equivalent export documentation with the contents of the shipment. Discrepancies in documentation, exports without a permit, or shipped to a consignee not listed on the permit, the use of an expired permit, among others, may result in a detention. Pending clarification, or if a violation has occurred, the goods may be seized. Such goods and technology are not exempt from controls and require a permit, either individual or general (GEP). Where goods and technology may be exported under a GEP, there is an obligation on the part of the exporter to cite the appropriate GEP number on the B-13A. Where the goods and technology are tendered for export without citing the appropriate permit number, they may be detained or seized.*

[54] *Ellsmore*, *supra* note 9 at 42.

[55] Patrick Gunning, "Distributing Encryption Software by the Internet: Loopholes in Australia Export Controls" (January 1998), online: University of South Wales, Faculty of Law Homepagehttp://www2.austlii.edu.au/itlaw/articles/Gunning_Encryption.html (date accessed: 30 May, 2005).

[56] *Ellsmore*, *supra* note 9 at 42.

[57] *Ibid.*

[58] (1982) 65 F.L.R. 260 [*Vickers*], as cited in *Ellsmore*, *supra* note 9 at 43.

[59] *Vickers*, *supra* note 58.

[60] *Ibid.*

[61] *Ibid.*, at 276.

[62] 50 A.L.R. 684 [*Toby*]. Also cited in *Ellsmore*, *supra* note 9 at 43.

[63] *Toby*, *ibid.*; cf. *Vickers v. Young* (1982), 65 F.L.R. 260 at 276.

[64] (1990), 97 A.L.R. 513 at 520 aff'd. 100 A.L.R. 125.

[65] [1996] 4 ALL E.R. 481 (C.A.).

[66] *Ibid.*, at 493, para. j.

[67] *EIPA*, *supra* note 3 at s. 52. Online: Department of Justice Canada http://laws.justice.gc.ca/en/E-19/notinforce.html.

[68] *Ibid.*, at s. 53(2).

[69] *Ibid.*

[70] *Ibid.*, at s. 54.

[71] *Ibid.*, at. s. 55.

[72] See *Bernstein v United States Department of Justice*, 922 F. Supp. 1426 (N.D. Cal. 1996) [*Bernstein*]. In this case an academic had to apply for a permit before publishing his cryptographic research.

[73] See generally RSA Laboratories, "Is RSA Patented?", online: RSA Security http://www.rsasecurity.com/rsalabs/faq/6-3-1.html (dated accessed: 30 May, 2005).

[74] RSA Laboratories, "Is DES Patented?", online: RSA Security http://www.rsasecurity.com/rsalabs/node.asp?id=2326 (date accessed: 30 May, 2005).

[75] RSA Laboratories, "What are the Important Patents in Cryptography?", online: RSA Security http://www.rsasecurity.com/rsalabs/node.asp?id=2324 (date accessed: 30 May, 2005).

[76] See Organisation for Economic Co-operation and Development, "OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security", online: Organisation for Economic Co-operation and Development http://www.oecd.org/document/42/0,2340,en_2649_201185_15582250_1_1_1_1,00.html.

[77] See generally Task Force on Electronic Commerce, Industry Canada, "A Cryptography Policy Framework for Electronic Commerce: Building Canada's Information Economy and Society", online: International Federation of Library Associations and Institutions http://www.ifla.org/documents/infopol/canada/crypte.pdf.

[78] A.R.W. Sharpe, "How Mathematics Saved the World: The Allies' Decryption Efforts During World War II". Written for Dr. David Beatty, History 3300 on January 25, 1998, Enigma, online: http://personal.nbnet.nb.ca/michaels/hist3300.htm (date accessed: 24 February, 2004).

[79] Communications Security Establishment, "An Overview of the History of Cryptology", online: Communications Security Establishment http://www.cse-cst.gc.ca/en/documents/about_cse/museum.pdf (date accessed: 30 May, 2005).

[80] Alfred J. Menezes, Paul van Oorschot & Scott A. Vanstone, *Handbook of Applied Cryptography*, (Boca Raton: CRC Press, 1997).

[81] Centre for Applied Cryptography Research Homepage, "Overview", online: Centre for Applied Cryptographic Research, University of Waterloo http://www.cacr.math.uwaterloo.ca/. (See also the 11th CACR Information Security Workshop & 3rd Annual Privacy and Security Workshop Privacy and Security: Totally Committed, 7-8 November, 2002, University of Toronto.)

[82] IBM, "Cryptographic Research Group", online: IBM http://www.research.ibm.com/security (date accessed: 30 May, 2005).

[83] Microsoft Research, "Cryptography", online: Microsoft Research http://research.microsoft.com/crypto/ (date accessed: 24 February, 2004).

[84] Grabow, C.G., "L-5-Changes in Cryptographic Export-Import Rules", (Paper presented at the 26th Annual Computer Security Conference, November 1999) [unpublished].

[85] *OECD*, *Cryptography Policy: The Guidelines and the Issues*, (OECD, 1998). See also online: http://www.oecd.org/document/11/0,2340,en_2649_201185_1874731_1_1_1_1,00.html (date accessed: 15 August, 2005) [*OECD*].

[86] Taskforce on Electronic Commerce, Industry Canada, *Cryptography Policy Framework For Electronic Commerce: Building Canada's Information Economy and Society*, (Industry Canada, 1998) at 15. Also online: Industry Canada http://www.ifla.org/documents/infopol/canada/crypte.pdf (date accessed: 30 May, 2004) at p. 15 *[Cryptography policy Framework].*

[87] *Ibid.*

[88] *Ibid.*, at 11.

[89] M. Harrop, AEPOS Technologies Corporation, "The Canadian Cryptography Industry: An Exploratory Review of Cryptography Companies in Canada, Report to Consultation Participants", released March 7, 2001 at 2 [*Harrop*].

[90] *Ibid.*

[91] AEPOS Technologies, "Cryptography Policy Discussion Paper: Analysis of Submissions" (June 11, 1998) [unpublished] [*AEPOS*].

[92] *Ibid.*, at 16. See also Canadian Association of Internet Providers' submissions in response to "A Cryptography Policy for Canada's Information Economy and Society" Notice No. IPPB–003-98 – Release of Public Discussion Paper on Setting a Cryptography Policy Framework for Canada, Publication Date: 1998-02-18, submitted 21 April, 1998 at 5; Canadian Bankers Association's submission to Industry Canada, "Review of a Cryptography Policy For Electronic Commerce", submitted April 1998 at 15; and Entrust Technologies Ltd. Response to "A Cryptography Policy Framework for Electronic Commerce — Building Canada's Information Economy and Society", submitted April 20, 1998 at 5.

[93] Honourable John Manley, "Canada's Cryptography Policy" (Presentation to the National Press Club, October 1, 1998), online: Industry Canada http://www.ic.gc.ca/cmb/welcomeic.nsf/503cec39324f7372852564820068b211/85256613004a2e17852566900050dfd5!OpenDocumentl (date accessed: 30 May, 2005).

[94] *Notice to Exporters*, *supra* note 17.

[95] *Ibid.*, at s. 1.

[96] *Ibid.*, at s. 6.

[97] See the heading: "Exemptions from Items 1150–1155 of the ECL" *supra* note 14.

[98] *Ibid.*

[99] See s. 15 of *Notice to Exporters*, *supra* note 17:

> **15.** The regulatory changes will be implemented in a manner that respects our national cryptography policy. This policy encourages the widespread use of strong encryption and growth of export markets for Canadian technologies.

[100] *Harrop*, *supra* note 89.

[101] *Ibid* at 12.

[102] M. Harrop, AEPOS Technologies Corporation "The Canadian Cryptography Industry Revisited, Report to Consultation Participants", dated March 31, 2002 at 5.

[103] Global Internet Liberty Campaign, "Cryptography and Liberty: An International Survey of Encryption Policy" (February 1998), online: Global Internet Liberty Campaign: http://www.gilc.org/crypto/crypto-survey.html (date accessed: 30 May, 2005).

[104] G. C. Grabow, "L-5 Changes in Cryptographic Export-Import Rules" (presented to 26th Annual Computer Security Conference, October 1992).

[105] [1989] 1 S.C.R. 927.

[106] [1995] 3 S.C.R. 199.

[107] (2002) 209 D.L.R. (4th) 549 (S.C.C.).

[108] Peter W. Hogg, *Constitutional Law of Canada*, loose leaf ed. (Scarborough: Carswell, 1991) at 40-9.

[109] *Bernstein*, *supra* note 72.

[110] 93 Cal. App. 4th 648 (C. A. 2001) [*DVD Copy Control*].

[111] In *Universal City Studios Inc. et al. v. Corley*, 273 F.3d 429, 438-439 (2nd Cir. 2001), the Court stated that a computer source code is computer language that can be read and understood by people: "source code has the benefit of being much easier to read (by people) than object code, but as a general matter, it must be translated back to object code before it can be read by a computer … Object code usually constitutes computer electrical charges the presence or absence of which is represented by strings of 1's and 0's". "The object code file contains a sequence of instructions that the processor can understand but that is difficult for a human to read or modify." (searchSMB.com, "object code", online: searchSMB.com http://searchsmb.techtarget.com/sDefinition/0,,sid44_gci539287,00.html (date accessed: 30 May, 2005). "This task [of translation from source to object code] is usually performed by a program called a compiler. Since computer languages range in complexity, object code can be placed on one end of a spectrum, and different kinds of source code can be arrayed across the spectrum according to the ease with which they are read and understood by humans." [*Universal*].

[112] *DVD Copy Control*, *supra* note 110 at 661.

[113] *Universal*, *supra* note 111.

[114] *Ibid*., at 445–47. See also *Bernstein*, *supra* note 109. See opposing arguments to the decision in this case: Katherine A. Moerke, "Free Speech to a Machine? Encryption Software Source Code Is Not Constitutionally Protected 'Speech' Under the First Amendment" (2000) 84 Minn. L. Rev. 1007 and Seth Hanson, "*Bernstein v. The United States Department of Justice*: A Cryptic Interpretation of Speech" (2000) B.Y.U.L. Rev. 663.

[115] *Hogg*, *supra* note 108 at para. 40.6(a). It is to be noted that in contrast to the United States, where prior restraints are almost always struck down, in Canada the standards of section 1 justification are applicable to prior restraints, and some prior restraints have been upheld.

[116] [1986] 1 S.C.R. 103.

[117] *Hogg*, *supra* note 108 at 35-16–35-17.

[118] Jason Kerben, "Comment, The Dilemma for Future Communication Technologies: How to Constitutionally Dress the Crypto-Genie" (1997) 5 CommLaw Conspectus 125 at 147, cited in Norman Andrew Crain, "Bernstein, Karn and Junger: Constitutional Challenges to Cryptographic Regulations" (1999) 50 Ala. L. Rev. 869 at 894 [*Crain*].

[119] *Ibid*., at 895.

[120] Brian Krebs, "New Encryption Regulations Take Effect", online: Computer User.com http://www.computeruser.com/news/00/10/20/news2.html (date accessed: 30 May, 2005).

[121] *Crain*, *supra* note 118.

[122] See *Ruby v. Canada (Solicitor General)* [2002] S.C.C. 75 for a recent decision considering the *Oakes* analysis as applicable to the national security objectives underlying the law enforcement and investigation exemption in the *Privacy Act*, R.S.C. 1985, c. P-21, sections 51(2)(*a*), (3).

[123] *Hogg*, *supra* note 108 at 35-21.

[124] What are the important patents in Cryptography? RSA Security Homepage online,http://www.rsasecurity.com/rsalabs/faq/6-3-5.html (date accessed: 30 May, 2005).

[125] Covers the DES cipher.

[126] This is the first patent covering a public-key cryptosystem. It describes Diffie-Hellman key agreement, as well as a means of authentication using long-term Diffie-Hellman public keys.

[127] The Hellman-Merkle patent covers public-key systems based on the knapsack problem and now known to be insecure. Its broader claims cover general methods of public-key encryption and digital signatures using public keys.

[128] This patent describes the RSA public-key cryptosystem as used for both encryption and signing. It served as the basis for the founding of RSADS.

[129] This patent describes the Fiat-Shamir identification scheme.

[130] This is the most prominent among a number describing the use of control vectors for key management. This patent describes a method enabling a description of privileges to be bound to a cryptographic key, serving as a deterrent to the key's misuse.

[131] This patent describes the GQ identification scheme.

[132] This patent covers the Digital Signature Algorithm (DSA), the algorithm specified in the Digital Signature Standard (DSS) of the U.S. National Institute of Standards (NIST).

[133] This patent covers systems in which keys are held in escrow among multiple trustees, only a specified quorum of which can reconstruct these keys.