UIC John Marshall Journal of Information Technology & Privacy Law

Volume 16
Issue 3 *Journal of Computer & Information Law - Spring 1998*

Article 1

Winter 1997

Cryptography and Liberty: An International Survey of Encryption Policy, 16 J. Marshall J. Computer & Info. L. 475 (1998)

Wayne Madsen

David L. Sobel

Marc Rotenberg

David Banisar

ARTICLES

CRYPTOGRAPHY AND LIBERTY: AN INTERNATIONAL SURVEY OF ENCRYPTION POLICY

by WAYNE MADSEN, DAVID L. SOBEL, MARC ROTENBERG, & DAVID BANISAR OF THE ELECTRONIC PRIVACY INFORMATION CENTER†

† Wayne Madsen was the principal researcher and writer of this Article. Assistance was provided by David L. Sobel, Marc Rotenberg, and David Banisar. This Article was produced on behalf of the Global Internet Liberty Campaign, a coalition of forty-one human rights, civil liberties, and computer user groups around the world. More information on The Electronic Privacy Information Center ("EPIC") is available at http://www.epic.org/. A grant from the Open Society Institute funded the research.

I. THE IMPORTANCE OF CRYPTOGRAPHY

Emerging computer and communications technologies are radically altering the ways in which individuals communicate and exchange information. Along with the speed, efficiency, and cost-saving benefits of the "digital revolution" come new challenges to the security and privacy of communications and information traversing the global communications infrastructure.

In response to these challenges, the security mechanisms of traditional paper-based communications media—envelopes and locked filing cabinets—are being replaced by cryptographic security techniques. Through the use of cryptography, communication and information stored and transmitted by computers can be protected against interception to a very high degree. Until recently, there was little non-governmental demand for encryption capabilities. Modern encryption technology was traditionally deployed most widely to protect the confidentiality of military and diplomatic communications.[1] With the advent of the computer

1. Encryption is a mathematical process involving the use of formulas (or algorithms).

revolution, and recent innovations in the science of encryption, a new market for cryptographic products has developed. Electronic communications are now widely used in the civilian sector and have become an integral component of the global economy. Computers store and exchange an ever-increasing amount of highly personal information, including medical and financial data. In this electronic environment, the need for privacy-enhancing technologies is apparent. Communications applications such as electronic mail and electronic fund transfers require secure means of encryption and authentication—features that can only be provided if cryptographic know-how is widely available and unencumbered by government regulation.

Governmental regulation of cryptographic security techniques endangers personal privacy. Encryption ensures the confidentiality of personal records, such as medical information, personal financial data, and electronic mail. In a networked environment, such information is increasingly at risk of theft or misuse. In the "Resolution in Support of the Freedom to Use Cryptography," members of the Global Internet Liberty Campaign ("GILC") noted that "the use of cryptography implicates human rights and matters of personal liberty that affect individuals around the world" and that "the privacy of communication is explicitly protected by Article 12 of the Universal Declaration of Human Rights, Article 17 of the International Covenant on Civil and Political Rights, and national law."[2]

II. ENCRYPTION AND HUMAN RIGHTS

In many countries around the world, human rights organizations, journalists, and political dissidents are the most common targets of surveillance by government intelligence, law enforcement agencies, and other non governmental groups.[3] In some countries, such as Honduras and Paraguay, the state-owned telecommunications companies are active participants in helping the security services monitor human rights advocates. These problems are not limited to developing countries. French counter-intelligence agents wiretapped the telephones of prominent journalists and opposition party leaders. The French Commission Nationale de Contrôle des Interceptions de Securité estimated that there are some 100,000 illegal taps conducted each year in France. There have been numerous cases in the United Kingdom which revealed that the British intelligence services monitor social activists, labor unions, and

2. *IP: Resolution in Support of the Freedom to Use Cryptography,* (visited March 12, 1998) <http://icg.stwing.upenn.edu/cgi-bin/mfs/02/3351.html>.

3. The United States Department of State, reported widespread illegal or uncontrolled use of wiretaps by both government and private groups in over 90 countries in *Country Reports on Human Rights Practices.*

civil liberties organizations. A recent United Kingdom bill was enacted that allows for the surveillance of lawyers and priests. In Germany, a bill is currently pending that would allow, for the first time since the Nazi era, the ability to wiretap journalists' offices. The European Parliament issued a report in January 1998 revealing that the United States National Security Agency was conducting massive monitoring of European communications.

Many human rights groups currently use encryption to protect their files and communications from seizure and interception by the governments they monitor for abuses. These countries include Guatemala, Ethiopia, Haiti, Mexico, South Africa, Hong Kong, and Turkey. Other groups such as Amnesty International U.S.A., also use cryptographic techniques to digitally sign messages that they send over the Internet to ensure that the messages are not altered in transmission.[4]

III. THE GLOBAL INTERNET LIBERTY CAMPAIGN AND ENCRYPTION

The Global Internet Liberty Campaign ("GILC") was established in June 1996 to protect civil liberties and human rights in the on-line world. Among the principles adopted by GILC was the belief that users of the Internet should have the right to "encrypt their communication and information without restriction."

In September 1996, GILC issued its "Resolution in Support of the Freedom to Use Cryptography" at an international conference sponsored by GILC in Paris. The resolution was addressed to the Organization for Economic Cooperation and Development ("OECD"). GILC urged the OECD to base its policies on "the fundamental rights of citizens to engage in private communications." Subsequent guidelines adopted by the OECD recognized that the "fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods."[5]

GILC continues to monitor activities concerning the freedom to use cryptography around the world. GILC maintains an extensive collection of resources about encryption policy at the GILC web site. Members of

4. *See Center for Science, Technology, & Congress* (visited March 12, 1998) <http://www.aaas.org/spp/dspp/cstc/briefings/crypto/dinah.html>. Additional information on the use of encryption technology by international human rights organizations is contained in the briefing paper *Encryption in the Service of Human Rights*, produced by Human Rights Watch.

5. *See infra* Part VI.B for a discussion of THE ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT: ("OECD") GUIDELINES ON CRYPTOGRAPHY POLICY.

GILC offer training in the use of cryptographic methods to human rights organizers, journalists, and political activists.

IV. PURPOSE OF THE SURVEY

The survey presented in this article was undertaken by the Electronic Privacy Information Center ("EPIC"), on behalf of GILC, to provide a comprehensive review of the cryptography policies of virtually every national and territorial jurisdiction in the world. Unlike previous surveys of international cryptography policy, the GILC survey is based on direct contact with over 200 nations and territories. Territories were included because their economic policies are often different from their mother countries.

EPIC sent letters to the embassies, United Nations missions, government ministries, trade boards, and information offices of some 230 countries and territories. The letters inquired about four major areas concerning cryptography policies:

1.) controls maintained by the governments on the domestic use of cryptography in their countries;

2.) controls maintained by the governments on the importation to their countries of computer programs or equipment that permit cryptography;

3.) controls maintained by the governments on the exportation of domestically developed computer programs or equipment that permit cryptography; and

4.) identification of the agency or department of the governments responsible for setting policy on the use, importation, or exportation of cryptographic technology.

EPIC referred to a preliminary survey commissioned by the United States National Institute of Standards and Technology ("NIST") in September 1993 that first attempted to collect information on the cryptographic policies of foreign countries.[6] This Report concentrated mainly on the policies imposed by the Cold War-Era Coordinating Committee on Multilateral Export Controls ("COCOM"), a grouping of Western nations that was abolished in 1994 and replaced by the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.[7]

---

6. The United States National Institute of Standards and Technology Survey on Encryption Policy (on file with the authors) [hereinafter NIST Survey].

7. These countries are Australia, Austria, Belgium, Canada, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Portugal, Spain, Sweden, United Kingdom, and United States. Others have subsequently acceded to the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.

EPIC also referred to a Report prepared by the United States Department of Commerce and the National Security Agency ("NSA") for the Interagency Working Group on Encryption and Telecommunications Policy, obtained by EPIC under the Freedom of Information Act.[8] The United States Department of Commerce and NSA attempted to obtain and analyze copies of the laws and regulations from as many encryption-producing nations as possible. The two agencies based some of their research on the NIST Survey, State Department messages from United States embassies abroad, and Reports from United States Foreign Commercial Service representatives to the Commerce Department's Bureau of Export Administration. However, much of the Report was based on personal interviews with foreign government representatives in the intelligence community.

Recognizing the problems encountered by the Commerce Department and NSA in their survey, EPIC determined that the best way to research cryptography polices around the globe was to directly contact the various embassies and diplomatic missions. The reasoning was that governments themselves are best able to authoritatively explain their policies, especially on such a technical area. EPIC patterned the survey after one conducted in 1989 by the Computer Science and Law Research Group ("GRID") of the University of Quebec, on behalf of the government of Canada, which analyzed the data protection policies and laws of over 150 countries, and additionally, EPIC consulted the Crypto Law Survey.[9]

V. SURVEY RESPONSES

A 100 percent response was the goal of EPIC's survey, but external events dictated some non-responses. For example, the Embassy of Cambodia in Washington, D.C. referred EPIC to the Ministry of Posts and Telecommunications in Phenom Penh, Cambodia. After sending a facsimile to the Ministry of Posts and Telecommunications, Cambodia was rocked by a coup d'etat. Several cabinet ministers fled or were executed, and no further information was forthcoming. A facsimile sent to the Finance Ministry of Montserrat in Plymouth, the island's capital, was shortly followed by the eruption of the Soufriere Hills volcano, which destroyed the capital city and sent most of the island's population into exile. Queries made to the embassies of Afghanistan, Congo (Brazzaville),

8. The United States Department of Commerce and the National Security Agency for the Interagency Working Group on Encryption and Telecommunications Policy International Encryption Report (on file with the authors) [hereinafter Commerce Department/ NSA Report].

9. *See Crypto Law Survey* (visited March 12, 1998) <http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm>. This survey includes descriptions of crypto policies in many of the world's countries as well as links to important source documents.

Congo (Kinshasa), Comoros, and Sierra Leone were not answered, likely due to the civil wars in those nations.

The signatories of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies ("Wassenaar Arrangement") served as a baseline for the determination of the cryptography export policies of some countries. By July 1996, the Wassenaar Arrangement was acceded to by thirty-one countries.[10] Bulgaria and Ukraine have also acceded to the Wassenaar Arrangement. The Wassenaar Arrangement controls the export of cryptography as a dual-use good, i.e., one that has both military and civilian applications. However, the Waasenaar Arrangement also provides an exemption from export controls for mass-market software. In addition, software containing cryptography may be subject to controls as a dual-use item. The confusion brought about by such a contradiction was apparent in the responses of some countries regarding their presumed obligations under the Waasenaar Arrangement.

Reported countries have been grouped into three categories regarding controls on cryptography. A *"green"* designation signifies that the country has either expressed support for the OECD Guidelines on Cryptography, which generally favor unhindered legal use of cryptography, or has no cryptography controls. A *"yellow"* designation signifies that the country has proposed new cryptography controls, including domestic use controls, or has shown a willingness to treat cryptographic-enabled software as a dual-use item under the Waasenaar Arrangement. A *"red"* designation denotes countries that have instituted sweeping controls on cryptography, including domestic use controls. Some countries do not fit neatly into one of the three categories, but trends may show them as being borderline, i.e., *"yellow/red."*

VI. SUMMARY OF RESULTS

EPIC found that most countries in the world today do not have regulations on the use of cryptography. In the vast majority of countries, cryptography may be freely used, manufactured, and sold without restriction. This is true for both leading industrial countries and for countries in emerging markets. Additionally, EPIC noted that recent trends in international law and policy suggest greater relaxation in controls on cryptography. The OECD Cryptography Policy Guidelines and the Ministerial Declaration of the European Union, both released in 1997, argue

10. The countries acceding to the Wassenaar Arrangement are Argentina, Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Poland, Portugal, the Republic of Korea, Romania, the Russian Federation, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States.

for the liberalization of controls on cryptography and the development of market-based, user driven cryptography products and services. These new multi-national agreements have implications for controls that currently restrict the use of cryptography. In France, for example, it is likely that domestic restrictions will be liberalized as French law is brought in line with the trade requirements of the European Union.

There are a small number of countries where strong domestic controls on the use of cryptography are in place.[11] There are an even smaller number of countries that are currently considering the adoption of new controls.[12]

The policies of the United States are the most surprising, given the fact that virtually all of the other democratic, industrial nations have few, if any, controls on the use of cryptography. The position may be explained, in part, by the dominant role that state security agencies in the United States hold in the development of encryption policy.

A. Survey Results

1. *Anguilla: Green*

Anguilla is a self-governing British territory in the Caribbean. It has also attracted an off-shore Internet industry which takes advantage of the territory's tax haven status. In an interview with Charles Platt from *Wired* magazine, Victor F. Banks, the Anguillan Minister of Finance, alluded to Anguilla as a base for Internet commerce. Mr. Banks stated:

> [h]ere in Anguilla we are well situated for Internet commerce. Our banks are well regulated, clean, secure; we are very vigilant against criminal activity; we have strong rules against money laundering and traffic in illegal drugs. We have mutual legal assistance with the [United States] that allows it to get information from us about any clientele involved in criminal activity, although it can't go on fishing expeditions to find out about tax avoidance.[13]

Offshore Information Services is one company that offers Anguilla domain name services (".ai"), e-mail accounts, virtual web sites, and links to encryption programs like Pretty Good Privacy ("PGP").[14] It also offers the opportunity to engage in cryptographic civil disobedience. One may send a three-line encryption program to Anguilla. In the United States, this simple harmless act is illegal, and is a violation of the Inter-

11. These include Belarus, China, Israel, Pakistan, Russia, and Singapore.

12. These include India, South Korea, and the United States.

13. *See* Charles Platt, *Plotting Away in Margaritaville*, Wired, July 1997.

14. Alan Freedman, The Computer Desktop Encyclopedia 657 (1996). An encryption program developed by Phil Zimmermann that is based on Rivest Shamir Adleman ("RSA") public-key cryptography.

national Traffic in Arms Regulations ("ITAR").[15] By hosting such an operation, Anguilla does not seem to be a country in support of United States initiatives on cryptography.[16]

2. *Antigua and Barbuda: Green*

The Embassy of Antigua and Barbuda in Washington, D.C. did not respond to our survey. However, perusal of their Free Trade Zone web site yielded the fact that the island nation is trying to compete with Anguilla in luring international data services, including those reliant on the Internet. Several virtual casinos have been established in the Free Trade Zone. It is certain that strong encryption is a high priority for such operations.

3. *Argentina: Yellow*

Argentina has acceded to the Wassenaar Arrangement and is presumably committed to restricting the export of cryptographic products and technology as dual-use goods.[17]

4. *Armenia: Yellow*

According to the Second Secretary of the Embassy of Armenia in Washington, D.C., Armenia does not currently have a policy on the use of cryptography. However, the Armenian government has recently set up a Department of Information and Publications that is planning to initiate legislation concerning the use of cryptography.[18]

5. *Australia: Green / Yellow*

The Embassy of Australia stated they had received EPIC's request for information on Australia's laws on the use, export, and import of cryptographic products, but were unsure of what agency of the Australian government to forward the request. EPIC informed the Embassy of Australia that the Attorney General's Department was most likely the agency possessing the information that EPIC desired. The confusion by the Embassy of Australia as to which government department is responsible for cryptography, was cited in the government-commissioned *Review of Policy Relating to Encryption Technologies*, authored by former deputy director of the Australia Security Intelligence Organization

15. *See ITAR Civil Disobedience* (visited March 12, 1998) <http://online.offshore.com.ai/arms-trafficker/>.

16. *See* Platt, *supra* note 13.

17. *See Firma Digital Centros de Interés y Material de Referencia* (visited March 12, 1998) <http://www.jus.gov.ar/firma/index.html>.

18. *See* Letter from Embassy of the Republic of Armenia (July 31, 1997) (on file with the authors).

("ASIO"), Gerald Walsh. In what is popularly entitled the Walsh Report (issued on October 10, 1996 and initially embargoed by the government for public release), Walsh criticizes the government for its lack of coordination in establishing a cryptographic policy: "[t]he Review found a lack of clarity as to which Minister and which department had responsibility for cryptography policy and the consequent danger of a lack of coordination in policy development. These deficiencies need to be overcome."[19]

The following is gleaned from the Commerce Department/NSA Report:

> Australian legislation controlling the export of cryptography products has existed since at least 1987 when Australia became a member of COCOM. Australian regulations, unlike COCOM, include all cryptographic products under a separate category rather than distinguishing them as dual-use or military. Cryptographic products require Ministry of Defense approval under Regulation 13B and the associated Schedule 13 of the Customs (Prohibited Exports) Regulations. As such, Australian export control regulations exceed both COCOM and Wassenaar guidelines in some areas, most notably in requiring individual export licensing for mass-market applications software and other mass-market software performing cryptographic functions.[20]

With COCOM's revision of the control lists in 1991, Australia adopted the revised lists that included the decontrol of mass-market cryptographic software. However, by November 1994, Australia had specifically excepted cryptographic software from the decontrol permitted by COCOM, again requiring individual licensing on such products. The Commerce/NSA Report redacts information from State Department Canberra cables explaining Australia's decision to re-impose individual licensing.[21]

According to the Australian Department of Foreign Trade, as referenced in State Department Canberra Cable 03283-93, Australia has a reasonably advanced commercial encryption industry, mainly focused on protecting commercial data flow via modems, voice scramblers, and mobile phones, and that Australian exports of such products are mainly to the financial industry.[22] Approval or denial of export applications is based on economic factors, the impact on Australian national security, and international obligations. Applications for export of cryptographic equipment are referred to the Defence Signals Directorate ("DSD") for technical advice on the impact of export on national security. DSD is the

19. *See* Gerald Walsh, *Review of Policy Relating to Encryption Technologies*, WALSH REPORT, Oct. 10, 1996.

20. *See* Commerce Department/NSA Report, *supra* note 8.

21. *Id.*

22. *See* United States Embassy State Department Canberra Cable 03283-93, Canberra, Australia (June 1995) (on file with the authors).

agency responsible for collecting foreign signals intelligence ("SIGINT"), much of which is shared with the United States National Security Agency under the terms of the United Kingdom-United States of America Security Agreement of 1948. DSD is also the agency responsible for the security of all Australian government communications.

In December 1996, Australia amended its export control laws to allow a personal-use exemption for encryption software that remains in the control of Australian users.

According to the Commerce/NSA Report, there are no import controls on cryptographic products in Australia.[23] Additionally, according to the Commerce/NSA Report, the private use of encryption devices is limited only by the requirement to obtain the Australian Telecommunications Authorities' ("Austel") approval for any equipment to be attached to the public switch telephone network.[24] Approval is generally granted provided the equipment does not harm the network. Australia does not appear to use homologation laws to control the private use of encryption. Homologation laws restrict Postal, Telegraph, and Telephone ("PTT")[25] customers from using telecommunications equipment on the network without first obtaining the consent of the PTT authority. Some governments use homologation regulations as a pretext to restrict the use of cryptography on telecommunications networks.

In August 1997, Senator Richard Alston, the newly-designated Federal Information Economy Minister, assumed responsibility for cryptography policy-making from the Attorney General's department. The Attorney-General's department was criticized for initially suppressing the Walsh Report on cryptography in early 1997.

It was reported that the new National Office for the Information Economy ("NOIE") would have "significant private sector input," including long and short-term contracts for staff from business backgrounds, in order to reflect corporate concerns.[26]

6. *Austria: Yellow*

The Embassy of Austria in Washington, D.C. informed EPIC that the Austrian organization responsible for cryptography usage and exports and imports was the Federal Ministry of Foreign Affairs, Section

---

23. *See* Commerce Department/NSA Report, *supra* note 8.

24. *See* Commerce Department/NSA Report, *supra* note 8.

25. ALAN FREEDMAN, THE COMPUTER DESKTOP ENCYCLOPEDIA 702 (1996). The governmental agency responsible for combined postal, telegraph and telephone services in many European countries.

26. Paul Montg, *Alston Claims C: New Office Wrests Control From Department* (visited March 4, 1998) <http://zdnet.com.au/pcweek/content/1001/pcoz0004.html>; *see also Review of Policy Relating to Encryption Technologies*, WALSH REPORT, Oct. 10, 1996.

VI, in Vienna, Austria. A facsimile to the Federal Ministry of Foreign Affairs agency went unanswered.

According to the Commerce/NSA Report, the Austrian government controls all encryption software as a dual-use item, and special licenses are required for its export, transit, or re-export.[27] The legislation governing dual-use items is the *Aussenhandelsgesetz 1995 Bundesgesetzblatt 172*, as well as accompanying *Bundesgesetzblatt 180/1995*. Licenses are denied to destinations where an armed conflict is ongoing, to countries of concern, and to those against which there are international sanctions.[28]

According to a study by the Institute for Applied Information Processing and Communication ("IAIK"), regulations concerning the use of cryptography within Austria are covered by the law on internal radio transmissions ("*Betriebsfunkverordnung—BFV* 1995"). Encryption is explicitly forbidden because frequencies assigned to certain companies and organizations are considered privileged frequency allocations that can only be used for company-specific internal communications. However, some frequencies are allocated to whole sectors of the economy resulting in the problem that competitors may listen to conversations. Consequently, there is a strong interest from affected companies to change these regulations. The only exceptions are the sub-units of the Ministry of Interior (mainly the police and security forces). Public communication systems may be encrypted. International regulations on amateur radio which demand transmission in clear text (and restrict content very strongly) are enforced in Austria.

On July 8, 1997, Caspar Einem, the Austrian Minister for Science and Transport, endorsed the communiqué of the European Ministerial Conference on Global Information Networks in Bonn, Germany. The communiqué stated the participating ministers "will work to achieve international availability and free choice of cryptography products and interoperable services, subject to applicable law." The ministers also declared that "if countries take measures in order to protect legitimate needs of lawful access, they should be proportionate and effective and respect applicable provisions relating to privacy." The ministers also took note of the recently agreed OECD Guidelines on Cryptography policy as a basis for national policies and international co-operation. The ministers also emphasized "the need for a legal and technical framework at European and international levels which ensures compatibility and

27. *See* Commerce Department/NSA Report, *supra* note 8.

28. *See* United States Embassy Commerce Department Vienna Cable 004611, Vienna, Austria (June 7, 1995) (on file with the authors).

creates confidence in digital signatures."[29]

7. *Bahrain: Unknown*

The Embassy of Bahrain in Washington, D.C. contacted EPIC via telephone and stated that the Directorate of Islamic Affairs, a component of the Ministry of Justice and Islamic Affairs, an agency in Manama, Bahrain was responsible for regulating the use of cryptography. A direct query to that agency went unanswered.

8. *Belarus: Red*

Belarus restricts the manufacture, maintenance, and use of cryptographic products. Licenses are required by the State Security Committee ("The Belarussian KGB").[30]

9. *Belgium: Green*

Belgium requires individuals wishing to export cryptography to countries other than the Netherlands and Luxembourg to first obtain an export license. However, the European Union ("EU") statutes have liberalized these requirements to cover additional EU members and certain non-EU countries.

In December 1994, the Belgian Parliament passed a law that required escrowed encryption. The law authorized the Belgian Institute for Posts and Telecommunications to establish a mandatory key escrow deposit system. The law contained homologation provisions that permitted the Belgacom, the Belgian PTT, to disconnect a phone that used unescrowed encryption. The regulations to enforce the law were never released and the law was repealed in December 1997.

On July 8, 1997, Jos Chabert, the Belgian Vice Premier and Minister for Economics for the Brussels Capital Region, endorsed the communiqué of the European Ministerial Conference on Global Information Networks in Bonn, Germany.[31]

---

29. Facsimile from Embassy of Austria, Office of the Commercial Counselor (June 24, 1997) (on file with the authors); *see also A Study of the International Market for Computer Software with Encryption*, <http://www.epic.org/crypto/export_controls/commerce_study_summary.txt> [hereinafter *International Market*].

30. *See International Market, supra* note 29.

31. *See id.*; *see also* Lambda Bulletin 2.05, *Belgium Discovers Strong Encryption Rules; France Will Adopt Electronic Locksmiths* (visited March 3, 1998) <http://www.freenix.fr/netizen/205-e.html>; Interdisciplinary Center for Law & Information Technology, *Papers, Documents and links*, (visited March 11, 1998) <http://www.law.kuleuven.ac.be/icri/papers/dutch_eng.htm>.

10. *Belize: Green*

The Embassy of Belize in Washington, D.C. informed EPIC that they were not aware of any laws in Belize concerning the use of cryptography. The Embassy of Belize informed EPIC that cryptography was under the jurisdiction of the Attorney General's Ministry in Belmopan.[32]

11. *Brazil: Green*

According to the 1993 NIST Survey, Brazil does not impose import restrictions for encryption technology.[33] The PGP encryption program in Portuguese is available from Brazil via the Internet.[34]

12. *Bulgaria: Green / Yellow*

Bulgaria has acceded to the Wassenaar Arrangement and is presumably committed to restricting the export of cryptographic-enabled software as a dual-use good.

On July 8, 1997, Antoni Slavinski, the Bulgarian President of the Committee of Posts and Telecommunications and Christo Balarev, the Bulgarian Deputy Minister of Education and Science, endorsed the communiqué of the European Ministerial Conference on Global Information Networks in Bonn, Germany.[35]

13. *Cambodia: Unknown*

The Embassy of Cambodia in Washington, D.C. informed EPIC that, although they were not aware of any laws concerning the use of cryptography in Cambodia, the Ministry with responsibility was the Ministry of Posts and Telecommunications in Phenom Penh, Cambodia. A facsimile to the agency was followed by a coup d'état and no further information was forthcoming.[36]

14. *Campione d'Italia: Green*

Campione d'Italia is a small Italian enclave on the shores of Lake Lugano. It is totally surrounded by Switzerland. Although technically part of Italy, Campione d'Italia's close affiliation with Switzerland, a non-member of the European Union, has made it a virtual "neutral zone" from European laws, including those dealing with taxation. A company developing encryption in this feudal anomaly would face little or no ex-

32. *See* Facsimile from Embassy of Belize (June 20, 1997) (on file with the authors).

33. *See* NIST Survey, *supra* note 6.

34. *See NIST Preliminary Results of Study of Non-U.S. Cryptography Laws/Regulations*, (visited Sept. 27, 1993) <http://www.dca.fee.unicamp.br/pgp>.

35. *International Market, supra* note 29.

36. *See* Facsimile from Royal Embassy of Cambodia (June 19, 1997) (on file with the authors).

port restrictions because Campione's border with Switzerland is open (there is also unrestricted access to Liechtenstein) and Swiss laws do not apply in the enclave. There is full Internet access via the modern Swiss PTT network. Because Campione has attracted numerous companies and banks, Italy prefers not to apply its laws to the territory.

15. *Canada: Green / Yellow*

According to the Commerce/NSA Report, the Export and Import Permits Act ("EIPA"), the Export Control List ("ECL") and the Area Control List ("ACL") are the mechanisms by which Canada controls exports.[37] The EIPA authorizes the Government to exercise export controls to ensure that military or strategic goods are not exported to destinations representing a strategic threat to Canada. The Ministry of External Affairs is responsible for implementation of the act.

Canada was a member of COCOM and continues to adhere to the Wassenaar Arrangement. Canada has, therefore, issued guidelines for the export of information security related equipment and technologies that are reflected in Group 1 of the Export Control List. Accordingly, export licenses are required for export to all destinations except the United States. The Foreign Affairs Export Controls Division works closely with Canada's Communications Security Establishment ("CSE"), the NSA's Canadian SIGINT partner, regarding export decisions on cryptographic products. The Division stated that the CSE works closely with the NSA, the United Kingdom's Government Communications Headquarters ("GCHQ"), and Australia's DSD on cryptographic export policies.

There are no import controls imposed by Canada and there are no laws restricting the private use of cryptography. Canada's homologation regulations require that cryptographic equipment conform to public network technical requirements.[38]

16. *China: Red*

According to the NIST Survey, China practices a licensing system for importing various commodities.[39] An application must be filed and a license obtained in advance by corporations approved by the State to engage in the business of importing commodities. The licenses are valid for one year and an application for extensions may made by corporations.

The Notice of the General Administration of Customs of the People's Republic of China, § 50-305, of November 1, 1987 (List of Prohibited and

37. *See* Commerce Department/NSA Report, *supra* note 8.

38. *See International Market*, *supra* note 29.

39. *See* NIST Survey, *supra* note 6.

Restricted Imports and Exports), restricts the importation of voice-encoding devices.

Corporations engaging in the exportation business must file an approval application with the Ministry of Foreign Trade or the foreign trade bureau of the particular province. The Ministry establishes an export control list of prohibited and restricted goods. These regulations are contained in Interim Procedures of the State Import-Export Commission and Ministry of Foreign Trade of the People's Republic of China Concerning the System of Export Licensing of June 3, 1980.[40]

17. *Croatia: Green*

The Croatian embassy in Washington, D.C. did not respond to our survey. However, it is noteworthy that the Cryptographic Reference Center's web page,[41] which is operated jointly by the Croatian Academic and Research Network ("CARNet"), and the Faculty of Electrical Engineering and Computing ("FER"), in Zagreb, Croatia, makes various cryptographic programs (e.g. PGP 5.0) available on-line.

There are no identifiable laws or regulations governing the import or use of cryptography in Croatia.

18. *Cyprus: Green / Yellow*

The Cypriot Embassy in Washington, D.C. did not respond to our survey. However, Cyprus endorsed an international statement on cryptography in July 1997. On July 8, 1997, Dinos Michaelides, the Cypriot Minister of the Interior, endorsed the communiqué of the European Ministerial Conference on Global Information Networks in Bonn, Germany.

19. *Czech Republic: Green / Yellow*

The Czech Republic has acceded to the Wassenaar Arrangement and is presumably committed to restricting the export of cryptographic-enabled software as a dual use good. However, according to the Commerce/NSA Report, multiple Czech firms are taking advantage of United States export control regulations to develop their own encryption software.[42]

There are no identifiable laws governing the import or domestic use of encryption in the Czech Republic. On July 8, 1997, Igor Nemec, the Czech Chairman of the Office for the State Information System and Emanuel Ondracek, the Czech Vice Minister for Education, Youth and Sport, endorsed the communiqué of the European Ministerial Conference

40. *See* NIST Survey, *supra* note 6.

41. *See Cryptographic Reference Center* (visited March 12, 1998) <http://pgp.rasip.fer.hr>.

42. *See* Commerce Department/NSA Report, *supra* note 8.

on Global Information Networks in Bonn, Germany.[43]

20. *Denmark: Green*

According to Commerce/NSA Report, Denmark controls the export and re-export of encryption software pursuant to the Wassenaar Arrangement.[44] There is no evidence that these regulations extend to mass-market software. A validated license is required for exports and to date, none have been denied. Denmark does not differentiate between encryption algorithms of varying strengths.

Denmark regulates the export of strategic goods under a Ministry of Industry executive order dated November 12, 1993. The central element of the executive order is the list of strategic goods that are subject to the export control policy and may only be exported when the Business Policy Ministry has issued a license. The list is composed of products under embargo from the four international control systems, the Missile Technology Control Regime, the Nuclear Nonproliferation Treaty, the Australia Group, and the Wassenaar Arrangement. The executive order has been subsumed by the European Union dual-use regulation.

Denmark administratively processes export requests through a board sponsored by the Business Policy Ministry composed of Confederation of Danish Industry representatives and financed by industry. The Confederation of Danish Industry Board stated in response to a query from the United States Department of Commerce that individual validated licenses are required for the export of cryptographic equipment and software.[45]

Denmark does not control the import of encryption software. The Commerce/NSA Report description of Danish domestic use controls is entirely redacted, a possible result of a classified explanation of Denmark's homologation regulations on its telecommunications network.[46]

In June 1996, the Danish Information Technology Security Council advocated no restrictions on the use of encryption in Denmark, including mandatory key escrow systems. The Council decided that existing judicial search orders were sufficient in gaining access to encryption keys (an opinion also evident in Australia's Walsh Report). The Council also requested the Minister of Research and Information Technology to submit to Parliament a Bill on Digital Signatures.

On July 8, 1997, Ms. Jytte Hilden, the Danish Minister of Research and Information Technology, endorsed the communiqué of the European

43. *See International Market, supra* note 29.

44. *See* Commerce Department/NSA Report, *supra* note 8.

45. *See* United States Embassy Commerce Department Copenhagen Cable 2717, Copenhagen, Denmark (May 31, 1995) (on file with the authors).

46. *See* Commerce Department/NSA Report, *supra* note 8.

Ministerial Conference on Global Information Networks in Bonn, Germany.[47]

21. *Estonia: Green*

Estonia maintains neither import nor export restrictions on cryptography. On July 8, 1997, Uno Veering, the Estonian Secretary of State, endorsed the communiqué of the European Ministerial Conference on Global Information Networks in Bonn, Germany.[48]

22. *European Union: Green / Yellow*

According to the Commerce/NSA Report, in 1992, the European Commission proposed a dual-use regulation as part of the progression to the free market.[49] Since military exports were linked to Member States' national security concerns, control of such exports was deemed to be a matter for individual states. However, with dual-use goods, it was argued that, while military uses were of a national interest, their civil use was in the purview of the European Commission.

Eventually, a compromise was reached. The European Union Dual-Use Regulation was agreed upon. The basis for the regulation was Article 113 of the Treaty of Rome and a Maastricht-based Common Foreign and Security Policy Joint Action with a series of annexes. The European Union's Dual-Use Regulation contains twenty-four articles and it entered into force on July 1, 1995. Council Decision No. 94/942/CFSP, with eight articles and five annexes, has been appended to the European Union Dual-Use Regulation.[50]

An October 8, 1997 Report by the European Commission's Directorate-General XIII, which is responsible for Telecommunications, Information Market and Exploitation of Research, took issue with the United States' policy of encouraging key escrow and recovery schemes. The Re-

47. *International Market*, *supra* note 29; *see also Press Release 27.05.97, No Regulation on Cryptography Now* (visited March 12, 1998) <http://www.fsk.dk/fsk/presse/970527.html>.

48. *See International Market*, *supra* note 29.

49. *See* Commerce Department/NSA Report, *supra* note 8.

50. The series of regulations, decisions, and annexes state that:

a.) All Member States recognize the same list of dual-use goods (generally based on the COCOM and the Wassenaar Arrangement lists), destinations, and guidelines;

b.) The majority of dual–use goods may require, at most, only a general authorization for shipment between member states (and for favored destinations outside the Union—Australia, Canada, Japan, Norway, Switzerland, and the United States);

c.) A common level of export control should exist throughout the Union; and

d.) An export license issued in one Member State shall normally be valid for the shipment of goods from another Member State.

Id.

port stated that "restricting the use of encryption could well prevent law-abiding companies and citizens from protecting themselves against criminal attacks," adding that key escrow systems "would not . . . totally prevent criminals from using these technologies."

On the issue of "back door" mechanisms giving law enforcement and intelligence agencies the right to read the plain text of encrypted messages, the Report states that if such systems are required they "should be limited to what is absolutely necessary."

The Report was sent by the European Commission to the major bodies of the European Union, including the European Parliament, the Council of Ministers, the Economic and Social Committee and the Committee of the Regions.[51]

23. *Falkland Islands: Green*

According to Mr. D. G. Lang, the Attorney General of the Falkland Islands, there are no laws in the sparsely populated British territory that specifically deal with the use of cryptography. Mr. Lang informed EPIC that, as Attorney General, he has legitimate concerns about the possible use of cryptography by criminal organizations in furtherance of international crime or terrorism. However, Mr. Lang stated that there is no organized crime on the Falkland Islands. Mr. Lang offered his belief that the Falkland Island government is committed to joining the international effort to combat organized crime, and if the international community were to launch an effort against the use of "uncrackable" cryptography, the Falkland Islands would unite in this effort.

According to the Attorney General, although the Falkland Islands has a Constitutional guarantee respecting the privacy of the individual, this guarantee falls short of an absolute guarantee of privacy. On a Constitutional rationale, an individual, in the Attorney General's opinion, would most likely be unsuccessful in challenging a future provision prohibiting or restricting his or her use of cryptographic techniques.

The Attorney General stated that cryptography is used in the Falkland Islands for both business and government operations. The Attorney General is not opposed to usage by such organizations, but merely the use of cryptography by criminals for criminal purposes.

Since United Kingdom laws do not automatically apply to the territories, the response of the Falkland Islands Attorney General is important in that it may mirror the policies of several of the United Kingdom's remaining territories, including Gibraltar, Bermuda, and the Cayman

51. *See International Market, supra* note 29; *see also Communication from the Commission to the European Parliament, The Council, The Economic and Social Committee and the Committee of the Regions Ensuring Security and Trust in Electronic Communication* (visited March 12, 1998) <http://www.ispo.cec.be/eif/policy/97503toc.html>.

Islands.[52]

24. *Finland: Green*

According to the Ministry of Trade and Industry of Finland:

1.) Finland has implemented no specific legislation on the domestic use of cryptographic software and hardware. There are no special permit requirements in this respect.

2.) Finland has implemented no specific legislation on the import of cryptographic software and hardware. There are no import license requirements.

3.) Finland's national legislation relevant to export controls are:
   a.) Act on the Control of Exports of Dual-Use Goods (562/96).
   b.) Decree on Export Control of Certain Goods (645/96).
   c.) Decision of the Ministry of Trade and Industry on the Goods and Technologies Subject to Export Licensing (645/96).

4.) The national legislation refers to the European export control systems which consists of two legal instruments:
   a.) Council Regulation (EC) No. 3381/94 of December 19, 1994 setting up a Community regime for the control of exports of dual-use goods, with amendment (EC) No. 837/95.
   b.) Council Decision 94/942/CFSP of December 19, 1994 on the joint action adopted by the council on the basis of Article J.3 of the Treaty on European Union concerning the control of exports of dual-use goods (with several amendments—the latest relevant amendment concerning the controls on intra-Community trade of cryptography is 97/419/CFSP of June 26, 1997).

The Regulation is directly applicable to all the Member States of the European Union. Finland's control lists concerning the export control of cryptographic software and hardware are identical to those agreed to in the Wassenaar Arrangement and the European Union Treaty. The only relevant difference to the controls maintained by the European Union is that Finland's national legislation also covers the export of services, including the transfer of intangible technology, e.g., via electronic mail.

5.) The government agencies responsible for setting policies on the use, importation, and exportation of cryptographic products include the Ministry of Trade and Industry and the Ministry for Foreign Affairs for export controls and electronic commerce, and the Ministry of Communications, and the Security Police ("SUPO") (a component of the Interior Ministry). The Ministry of Finance has initiated a survey on the need for national information security legislation, including a law on digital signatures.[53]

52. *See* Letter from Attorney General of the Falkland Islands (July 3, 1997) (on file with the authors).

53. *See* Facsimile from Ministry of Trade and Industry, Helsinki, Finland (July 28, 1997) (on file with the authors).

It is noteworthy to point out the significant differences between the Ministry of Trade and Industry stated policy and that found in the Commerce/NSA Report. The Report states that "an individual validated license is required to import encryption software."[54] Additionally, the Commerce/NSA Report states that "Finland regulates the domestic use of cryptography."[55] Based on information contained in State Department Cable No. 3313, May 26, 1995, from the United States Embassy in Helsinki, the Report states that "export and import regulations on encryption software are not rigorously enforced in Finland."[56]

On July 8, 1997, Jan Store of the Finnish Foreign Ministry, endorsed the communiqué of the European Ministerial Conference on Global Information Networks in Bonn, Germany.[57]

25. *France: Red/Yellow*

The Embassy of France in Washington, D.C. informed EPIC that the *Service Central de la Sécurité des Systèmes d'Information* ("SCSSI") is the regulatory body in France with regard to cryptography. SCSSI reports directly to the office of the Prime Minister of France. EPIC contacted SCSSI in order to ascertain the laws on exports, imports, and domestic usage controls. No response was received by SCSSI.

The Commerce/NSA Report states that "France has the most comprehensive cryptologic control and use regime in Europe, and possibly worldwide."[58] France enacted a new law (Law No. 90-1170 of December 29, 1990) regulating the telecommunications industry.[59] Article 28 of Law No. 90-1170 specifically addresses encryption and adopts a control and export regime that is far more restrictive than that applied by the Wassenaar Arrangement and its predecessor, COCOM.[60] Law No. 90-1170, in order to "preserve the interests of national defense and of internal or external State security" regulates the "supply, export, or use of cryptologic methods or devices."[61] Therefore, although foreign cryptographic products may be imported into France without a license, they may not be supplied to French users nor used in France without authorization by the Prime Minister.

Based on Decree 92-1358 of December 28, 1992, cryptographic

54. *See* Commerce Department/NSA Report, *supra* note 8.

55. *See* Commerce Department/NSA Report, *supra* note 8.

56. *See* United States Embassy State Department Cable No. 3313, Helsinki, Finland (May 26, 1995) (on file with the authors).

57. *See id.*

58. *See* Commerce Department/NSA Report, *supra* note 8.

59. *See* Law No. 90-1170 of December 29, 1990.

60. *See id.*

61. *See id.*

equipment is separated into two categories.[62] The first category includes equipment which "can have no other purpose than authenticating a communication or ensuring the integrity of a transmitted message."[63] Such equipment requires the submission of a statement or declaration to SCSSI.[64] SCSSI routinely allows the supply and use of authentication equipment for use within France and also for export with a minimum of red tape.[65] However, the statement or declaration submitted for supply, use, or export of these devices must provide a "description of the security functions or mechanisms, including a detailed description of the cryptologic algorithm(s) (mathematical formulae) used and the system for the creation, development, and protection of the secret conventions; the software must be provided . . . in the source language."[66]

The second category includes cryptographic methods or devices, which provide for the confidentiality of data or transmissions and cryptologic analysis methods.[67] Supply, use, or export of devices in this category requires prior authorization.[68] The authorization, if provided, will either be a general authorization (i.e., an authorization to supply or export devices to any user) or a private use authorization which restricts supply, export, or use to specifically named individuals or communities.[69] Data that is submitted by the supplier, user, or exporter in order to obtain such authorization is extensive.[70] In general, the information submitted must "describe not only the algorithm for generating a sequence or pseudo-random block, but all the hardware or software facilities, transforming an intelligible plain signal into an unintelligible cryptogram, including generating keys, storing [the keys], [and] managing [the keys] . . . ."[71]

As far as importing and using cryptography in France is concerned, there are no restrictions on imports of encryption technology. However, the use and sales must be authorized either through a license application or by a declaration to the office of the Prime Minister, i.e., SCSSI. Users importing encryption software must register the encryption keys with the French government.

On June 18, 1996, the French legislature passed a new law on cryptography, *Loi de réglementation des télécommunications*, which amended

62. *See* Decree 92-1358 of December 28, 1992.
63. *See id.*
64. *See id.*
65. *See id.*
66. *See id.*
67. *See id.*
68. *See id.*
69. *See id.*
70. *See id.*
71. *See id.*

the 1990 law. The law slightly liberalized the use of authentication-only encryption but also introduced the requirement for trusted third party ("TTP") systems. However, the law was never enacted and the new Socialist government of Prime Minister Lionel Jospin seemed to change course on France's strict policies on cryptography usage. On August 29, 1997, the French Secretary of State for Industry Christian Pierret stated that France would liberalize its encryption policies. The liberalization of encrypting technology allows French companies to completely enter the market of electronic commerce currently dominated by United States companies.

On July 8, 1997, Christian Pierret endorsed the communiqué of the European Ministerial Conference on Global Information Networks in Bonn, Germany.[72]

26. *Federal Republic of Germany: Green*

According to the Embassy of the Federal Republic of Germany in Washington, D.C. in Germany there are:

1.) no controls on the use of encryption software or hardware;
2.) no controls on the import of encryption;
3.) export controls on encryption are comparable to those of the United States as they existed until early in 1997; and
4.) export controls are overseen by the Federal Exports Office of the Ministry of Economics.

According to the Commerce/NSA Report, export licenses are actually approved by the *Bündesamt fur Sicherheit der Informationstechnik* ("BSI"), the German Federal Information Security Agency, a department of the Ministry of the Interior.[73] The BSI coordinates with the *Bündesnachrichtendienst* ("BND"), the Federal Intelligence Service, a department of the Ministry of Defense, which provides the Defense opinion on the export in question.

German Economics Minister Guenter Rexrodt stated to the July 8, 1997 European Ministerial Conference on Global Information Networks in Bonn, which was attended by the European Union, Russia, Japan, Canada, and the United States, that Germany favors keeping software encryption unregulated. Guenter Rexrodt, Dr. Wolfgang Botsch, the Federal Minister of Post and Telecommunications, Dr. Jurgen Ruttgers, the Federal Minister for Education, Science, Research, and Technology, and Edzard Schmidt-Jortzig, the Federal Minister of Justice, endorsed the communiqué of the ministers conference.

---

72. *See International Market*, *supra* note 29; *see also* Global Information Networks, *French Leaders Urge Catch-up on Internet*, ZDNET NEWS (Aug. 29, 1997).

73. *See* Commerce Department/NSA Report, *supra* note 8.

Germany passed the Digital Signature Law ("SigG") on June 11, 1997. The digital signature system mandated asymmetric encryption. This system requires a secret key to be held by the signer and a public key that is certified by a trusted third party. The encryption algorithm to be used is not defined in the law. A separate Digital Signature Ordinance will most likely specify the algorithm. The law does not specify trusted third parties, but it requires that such parties be licensed by the government communications authority. This authority will certify trusted third parties and create a digital chain of trust for purposes of public key verification.[74]

27. *Gibraltar: Green*

The Gibraltar Government Mission in Washington, D.C. did not respond to our survey. However, the government of this British self-governing territory on the southern tip of Spain hosts an Internet gaming site ("InterKeno"). Registration is made via the Internet, and credit card details are submitted on heavily encrypted pages. The government of Gibraltar receives licensing fees from this operation and it is doubtful that they would support a form of key recovery or escrow that might result in disruption of the gaming operations.[75]

28. *Greece: Green / Yellow*

According to the Embassy of Greece in Washington, D.C., Greece has no current or projected legislation concerning the use, import, or export of cryptography. It is obvious that the Greek Embassy is not aware of Greece's presumed obligations to the European Union and the Wassenaar Arrangement governing exports of mass market cryptography software as a dual-use item.[76]

On July 8, 1997, Charalambos Katanidis, the Greek Minister of Transport and Communications and Emmanuel Fragoulis, the Greek Secretary General for Research and Technology, endorsed the communiqué of the European Ministerial Conference on Global Information Networks in Bonn, Germany.[77]

---

74. *See International Market, supra* note 29. *See also 7.1 Germany - Law on Digital Signatures Approved* (visited March 12, 1998) <http://www2.echo.lu/legal/en/news/9709/capter7.html#1>.

75. *See About the Games et al.* (visited March 11, 1998) <http://www.bet4abetterworld.com/general/geninfo.html#Security Information>.

76. *See also* the Survey Results entry for *Mount Athos, Republic of: Green.*

77. Letter from Embassy of Greece (July 15, 1997) (on file with the authors).

29. *Hong Kong: Yellow*

Import and export of cryptography is regulated by the Import and Export ("Strategic Commodities") Regulations. Licenses are required for cryptography imports and exports. Authentication cryptography that is not used for confidentiality purposes is exempt from this requirement.

It is uncertain whether China's strict import—export controls on cryptographic products have been or will be extended to Hong Kong. Such a development would severely restrict Hong Kong's manufacture and export of GSM cellular telephones with their built-in encryption capabilities. Under the British administration, there was little regulation of the telecommunications and Information Technology sectors.

30. *Hungary: Green / Yellow*

Hungary has acceded to the Wassenaar Arrangement and is presumably committed to restricting the export of cryptographically-enabled mass market software as a dual-use item.

On July 8, 1997, Dr. Karoly Lotz, the Hungarian Minister of Transport, Telecommunications and Water Management, endorsed the communiqué of the European Ministerial Conference on Global Information Networks in Bonn, Germany.

31. *Iceland: Green*

There are no restrictions on import, export, or domestic use of cryptography in Iceland. On July 8, 1997, Sveinn Thorgrimsson, the Icelandic Minister of Commerce and Industry, endorsed the communiqué of the European Ministerial Conference on Global Information Networks in Bonn, Germany.[78]

32. *India: Yellow / Red*

According to the Commerce/NSA Report, India has a formidable government structure that has exercised a great deal of control regulating foreign trade in items in short supply, rather than controlling defense-related exports for national security reasons.[79] As of May 1994, India had no publicly available guidelines or formal licensing procedures governing exports of munitions or sensitive dual-use commodities. It was felt that all munitions and military items of concern were produced by defense factories that restricted their export. Therefore, India maintained no formal export licensing system for munitions items. In March 1995, India published a list of strategic raw materials and technologies that are subject to export licensing. The list controls equipment and

78. *See International Market, supra* note 29.

79. *See* Commerce Department/NSA Report, *supra* note 8.

software for encrypted telemetry systems only (missile technology controls form a major portion of the list). No encryption software is controlled by the list.[80]

Under an Indo-United States memorandum of understanding on trade in sensitive technologies, the government of India has agreed to "facilitate" the import of items appearing on the United States Commodity Control List and the United States Munitions List. No information is available on Indian import or domestic use controls for cryptography.[81]

33. *Indonesia: Yellow*

According to the Embassy of Indonesia in Washington, D.C., cryptography regulations for domestic use are an entirely new matter for that country. The Commercial Attaché in Washington, D.C. has been keeping its parent organization in Jakarta, Indonesia informed of developments on the cryptographic front in the United States.

The embassy also informed EPIC that the agency responsible for setting policy on cryptographic exports and imports is the Directorate General of International Trade, a component of the Ministry of Industry and Trade.[82]

34. *Iran: Unknown*

The Interests Section of Iran at the Embassy of Pakistan in Washington, D.C. informed EPIC that our request for information on encryption laws in Iran had been forwarded to "the appropriate organization in the Islamic republic of Iran to be reviewed." No further information was forthcoming.[83]

35. *Ireland: Green/Yellow*

Ireland has acceded to the Wassenaar Arrangement and is presumably committed to restricting the export of cryptographic-enabled software as a dual-use item. However, Ireland facilitates the downloading of PGP via the Internet.[84]

A letter from the Irish Development Agency dated February 21, 1994, stated that Ireland does not impose any export restrictions on com-

80. United States Embassy State Department New Delhi Cable 8364, New Delhi, India (May 24, 1994) (on file with the authors); United States Embassy State Department New Delhi Cable 5852, New Delhi, India (May 3, 1995) (on file with the authors).

81. *See International Market*, *supra* note 29.

82. *See* Letter from Embassy of the Republic of Indonesia, Office of the Commercial Attaché (July 7, 1997) (on file with the authors).

83. Interests Section of the Islamic Republic of Iran, Embassy of Pakistan, Washington, D.C. letter dated July 7, 1997.

84. *See Pretty Good Privacy* (visited March 10, 1998) <http://www.efi.ie/pgp/welcome.html>.

puter software. Therefore, the Irish Development Agency stated this was the reason that "over 75 overseas software companies" had established operations in Ireland.

On July 8, 1997, Ronald Long, the Irish Assistant Secretary of Enterprise and Employment, endorsed the communiqué of the European Ministerial Conference on Global Information Networks in Bonn, Germany.[85]

36. *Israel: Red*

According to the Commerce/NSA Report, Israel, similar to France, has enacted comprehensive regulations regarding the export, import, and domestic use of encryption products under a Court Order entitled "The Supervision On Products and Utilities, (Dealing With Encryption Means), 1974, based upon the Supervision on Products and Utilities Law of 1957."[86] The court order states that a person will not engage in encryption activities, to include import, export, production or use, unless he or she is licensed by a national manager appointed by the Minister of Defense.

> According to State Department Tel Aviv Cable 11049-93:
> regulation of import and export of encryption devices and development of encryption technologies is handled by the Ministry of Defense, the same as the export of arms. Encryption exports must receive an export license specifying the end-user. A company wishing to develop encryption technology must first receive a license from the Ministry of Defense.[87]

37. *Italy: Green / Yellow*

According to the Commerce/NSA Report, Italy has two distinct laws regulating the export of cryptographic equipment.[88] The first law, Law No. 185/90 of July 9, 1990, regulates the export of cryptographic equipment as an armament of war and requires approval for all such equipment. This law requires the corporation requesting to export equipment, to seek approval from the Ministry of Foreign Affairs as well as the Ministry of Defense/Chief of Staff for Defense. Law No. 222/92 of February 27, 1992, and its supplement, Law No. 114/94 of May 18, 1994, also control the export of cryptographic equipment. They essentially implement COCOM, and the Wassenaar Arrangement guidelines. Although the Ministry of Foreign Trade has principal administrative authority in this

85. Letter from Irish Development Agency to Mr. Will Dwyer of Drath and Dwyer (Feb. 21, 1994) (on file with the authors).

86. *See* Commerce Department/NSA Report, *supra* note 8.

87. *See* United States Embassy State Department Tel Aviv Cable 11049-93, Tel Aviv, Israel (May 1995) (on file with the authors); *see also International Market, supra* note 29.

88. *See* Commerce Department/NSA Report, *supra* note 8.

area, decisions on export are made by an inter-Ministry commission that includes members from the Ministry of Foreign Affairs, Ministry of Defense, Ministry of Interior, and the Intelligence Services. Licenses are approved or denied based upon economic considerations, Italian national security, and international commitments.

The second law, Law No. 222/92 of February 27, 1992 implies that there is no registration requirement in Italy for manufacturers of encryption products. Although the law allows for general licenses for certain products and destinations, this is not applicable to cryptographic products, where, if the product is controlled, an individual license is required for all destinations. Italy complies with the General Software Note which decontrols mass-market software, however, this note only applies to general-purpose software (i.e., word processors, databases, etc.) and not to security-specific software. The majority of exports of cryptographic products from Italy are to financial institutions in Western Europe and Latin America.[89]

The Italian Parliament passed Law No. 59/97 of March 15, 1997. Article 15(2) of the Law No. 59/97 of March 15, 1997 establishes framework for electronically signed documents using digital signatures. The digital signature system uses asymmetric encryption. The technical standards on the encryption keys were to be implemented under a separate provision within 180 days of the draft regulation coming into force. Certificate authorities are to be licensed by the government and escrowed keys are to be held by notaries public.

There are no import control laws for cryptography nor are there any laws governing the domestic use of encryption.[90] On July 8, 1997, Pier Luigi Bersani, the Italian Minister of Industry, Commerce, and Handicrafts and Antonio Maccanico, the Italian Minister of Post and Telecommunications, endorsed the communiqué of the European Ministerial Conference on Global Information Networks in Bonn, Germany.[91]

38. *Japan: Yellow*

According to the Commerce/NSA Report, Japan regulates the export of encryption products according to the Foreign Exchange Foreign Trade Control Law, Japanese Law No. 416 of 1992, art. 15, no. 7 of the Export Trade Control Order and the Foreign Exchange Control Order.[92] These Cabinet Orders implement COCOM and Wassenaar Arrangement guide-

89. United States Embassy State Department Rome Cable 08436-93, Rome, Italy (July 7, 1995) (on file with the authors).

90. *See also* the Survey Results entry for *Campione d'Italia: Green.*

91. *International Market , supra* note 29; *see also European Commission Legal Advisory Board* (visited March 10, 1998) <http://www2.echo.lu/legal/en/news/9710/chapter7.html#2>.

92. *See* Commerce Department/NSA Report, *supra* note 8.

lines on encryption and include the General Software Note decontrolling mass-market products.

According to the Ministry of International Trade and Industry ("MITI") there are no import restrictions on cryptographic equipment in Japan. There are no domestic restrictions on the private use of cryptography in Japan. However, the Ministry of Posts and Telecommunications is responsible for regulating private and commercial encryption usage on the national telecommunications network.

On June 24, 1997, *Nikkei America* reported that MITI tightened export inspections for products using cryptography. MITI initiated stricter export inspection of products incorporating cryptographic technology. MITI announced that it would inspect such items with particular attention on national security issues and prevention of terrorist activities. The new policy has reduced the trading volume of computers, software and integrated circuit ("IC") cards. It became necessary for exporters to get MITI permission to export products using cryptography. The inspection time has increased from a few weeks to over a month, and MITI started stricter inspection after the United States government revised its regulations in October 1997. MITI changed the minimum product price requiring inspection from more than 1,000,000 yen to 50,000 yen.[93]

39. *Korea, Republic of: Yellow*

The Republic of Korea is a signatory to the Waasenaar Arrangement and is presumably committed to restricting the export of cryptographic-enabled software as a dual-use item. There appears to not be domestic controls on cryptographic-enabled software use.[94]

40. *Kuwait: Unknown*

The Embassy of Kuwait in Washington, D.C. informed EPIC that the Kuwait Information Office in Washington, D.C. had the information on cryptography regulations that EPIC requested. EPIC contacted the Kuwait Information Office and no further information was forthcoming.[95]

41. *Latvia: Green*

There are no restrictions on the import, export, and use of cryptography in Latvia. On July 8, 1997, Dr. Andris Virtmanis, the Latvian Min-

93. *See International Market , supra* note 29; *see also MITI Tightens Export Inspections for Products Using Cryptography* (visited March 10, 1998) <http://www.jya.com/mitizeal.txt>.

94. PGP is publicly available in Korean from <http://esperosun.chungnam.ac.kr/~hdpark/PGP/>.

95. *See* Letter from Embassy of Kuwait (Aug. 4, 1997) (on file with the authors).

ister of Transport, endorsed the communiqué of the European Ministerial Conference on Global Information Networks in Bonn, Germany.[96]

42. *Liechtenstein: Green*

Liechtenstein is a noted tax haven on the Swiss-Austrian border. This country is not member of the European Union. Liechtenstein maintains strict confidentiality controls on banking and company information held by its firms. Although Liechtenstein did not respond to the letter sent to its United Nations Mission, its banking laws give incite with regard to third-party encryption holders. According to Liechtenstein's laws, country authorities will not assist third party inquiries relating to foreign tax obligations.

43. *Lithuania: Green*

According to the Embassy of Lithuania in Washington, D.C., there are no laws in Lithuania governing the use, export, or import of cryptography. The Lithuanian Parliament network was queried for information for any proposed legislation. The results were negative. The Embassy informed EPIC that the policies on the use of cryptography in Lithuania would normally come under the jurisdiction of the Ministry of Communications and Informatics in Vilnius.

On July 8, 1997, Rimantas Pleikys, the Lithuanian Minister of Communications and Informatics and Vaidotas Blaziejus Abraitis, the Lithuanian Vice Minister of Communications and Informatics, endorsed the communiqué of the European Ministerial Conference on Global Information Networks in Bonn, Germany.[97]

44. *Luxembourg: Green / Yellow*

Luxembourg has acceded to the Wassenaar Arrangement and is presumably committed to restricting the export of cryptographic-enabled software as a dual-use item.

On July 8, 1997, Mady Delvaux-Stehres, the Luxembourg Minister of Social Security, Transport, and Communications, endorsed the communiqué of the European Ministerial Conference on Global Information Networks in Bonn, Germany.[98]

---

96. *See Computer Law and Legislature in Particular European Countries* (visited March 12, 1998) <http://www.ja.net/CERT/SIRCE/legislature.html>.

97. Facsimile from Embassy of the Republic of Lithuania (June 30, 1997) (on file with the authors).

98. *International Market*, *supra* note 29.

45. *Malaysia: Yellow*

There are no import or export controls on cryptography in Malaysia. However, in May 1997, the Malaysian parliament passed a law on digital signatures that provides a framework of legal certainty for electronic transactions. The law provides for key verification and deposit of public keys with trusted third parties. The government licenses the trusted third parties. The law does not specify the technical details for the key escrow system.[99]

46. *Mexico: Green*

According to the NIST Survey, the Mexican Institute of Foreign Trade governs imports and exports in Mexico.[100] However, no export or import controls were found to cover encryption technology.[101]

47. *Mount Athos, Republic of: Green*

The Republic of Mount Athos is a self-governed part of the Greek state subject to the Ministry of Foreign Affairs in its political aspect, and to the Ecumenical Patriarch of Constantinopole ("Istanbul") as regards its religious aspect. It is quasi-Greek Orthodox Vatican City without the diplomatic recognition and without the same degree of independence.

The Republic of Mount Athos has taken an aggressive stance against Pan-European law enforcement measures and agreements. The monks who live in the monastic Republic of Mount Athos are strongly committed to personal privacy. The republic's unique status could make it a cryptographic safe haven in Europe. On June 5, 1997 representatives from twenty monasteries of The Republic of The Republic of Mount Athos held a meeting to express their views, prior to the Greek Parliament's on the ratification of the Pan-European Schengen Agreement on law enforcement. If Greek Parliment attempted to implement the Pan-European Schengen Agreement, the representatives stressed that Greece would find itself in conflict with The Republic of Mount Athos' monks.[102]

---

99. *See Digital Signature Bill 1997* (visited March 12, 1998) <http://www.geocities.com/Tokyo/9239/digisign.html>; *see also Malaysia—New law on digital signatures passed* (visited March 12, 1998) <http://www2.echo.lu/legal/en/news/9709/capter7.html#2>.

100. *See* NIST Survey, *supra* note 6.

101. *See generally supra* note 11.

102. ATHENS NEWS AGENCY BULL. (No 1202), June 3, 1997; *see also Mount Athos* (visited March 12, 1998) <http://www-media.dbnet.ece.ntua.gr/Athos.html>.

48. *Nauru: Green*

Nauru is an independent island in the central Pacific that is eight square miles with a population of 8,000 individuals. According to the Honorary Counsel of Nauru in the United Kingdom, there are no applicable laws in Nauru governing the use, import, or export of cryptography. The responsible office for determining future policies is the Secretariat for External Affairs in Nauru.[103]

49. *Netherlands: Green/Yellow*

According to the Commerce/NSA Report, The Import and Export Act of 1963 serves as the basis for export regulations in the Netherlands.[104] Specific regulations are found in the Decree on Export of Strategic Goods and its Annex which implements the Wassenaar Arrangement and the strategic control lists. The Ministry of Economic Affairs is the principal agency in charge of licensing and enforcement of export controls. The export of cryptographic equipment from the Netherlands requires an individual license for all nations except Belgium and Luxembourg.

The National Communications Security Agency ("NCSA") has the responsibility for the determination regarding the impact on national security for any specific export of cryptographic equipment. The Commerce/NSA Report heavily redacts further information on the activities of NCSA, although it is known that this agency performs many of the functions of the NSA.[105]

There are no import restrictions for cryptographic products. The Commerce/NSA Report redacts information on the domestic use prohibitions in the Netherlands.[106] This is most likely a result of a classified description of the homologation tactics employed by the Netherlands PTT in restricting encryption from the national public communications network.

In March 1994, the Netherlands advanced a parliamentary bill that would have prohibited the possession, use, and marketing of powerful encryption products without a license. Due to an aggressive national reaction, the bill was withdrawn.

On July 8, 1997, Mrs. Annemarie Jorritsma-Lebbink, the Dutch Minister of Transport, Public Works, and Water Management and Dr. Hans Wijers, the Dutch Minister of Economic Affairs, endorsed the communiqué of the European Ministerial Conference on Global Information

103. *See* Facsimile from Republic of Nauru Honorary Counsel, Sevenoaks, United Kingdom (June 27, 1997) (on file with the authors).

104. *See* Commerce Department/NSA Report, *supra* note 8.

105. *See* Commerce Department/NSA Report, *supra* note 8.

106. *See* Commerce Department/NSA Report, *supra* note 8.

Networks in Bonn, Germany.[107]

50. *Netherlands Antilles: Green / Yellow*

The Cabinet Minister for the Netherlands Antilles informed EPIC that the Department of Justice of the Netherlands Antilles located in Willemstad, Curaçao had responsibility for establishing a policy on the use of cryptography.[108]

51. *New Zealand: Green / Yellow*

According to the Commerce/NSA Report, New Zealand treats encryption software as a dual-use item and requires an export license.[109] The governing legislation is the Export Prohibition Regulations of 1953 and the Customs Act of 1966. Export permits are issued by the Customs Department on the advice of the Ministry of Foreign Affairs and Trade ("MFAT"). The Customs Act of 1966 Section 54, states that "[t]he Governor-General may from time to time, by Order in Council, prohibit the exportation from New Zealand of any specified goods or goods of a specified class or classes" (followed by a list of specific conditions on prohibitions). The Commerce/NSA Report fails to mention the influence of the Government Communications Security Board ("GCSB") in approving encryption exports.[110] The GCSB is the NSA's equivalent and partner in New Zealand. The entity within MFAT which handles export controls is the International Security and Arms Control Division ("ISACD"). ISACD is advised by GCSB.

The New Zealand government relies on the United States government's export policies as a guideline for acceptability. No formal licenses have been denied recently, although some license requests have been informally discouraged. New Zealand has no controls over importation or domestic use of encryption software.[111]

52. *Nicaragua: Unknown*

EPIC was informed that the Center for Exports and Imports ("CEI") in Managua, Nicaragua was responsible for cryptography exports and imports in Nicaragua. Follow-up correspondence with that agency yielded no further information.[112]

---

107. *See International Market, supra* note 29.

108. *See* Facsimile from Het Kabinet Van De Gevolmachtigde Minister Van De Nederlandse Antillen (June 30, 1997) (on file with the authors).

109. *See* Commerce Department/NSA Report, *supra* note 8.

110. *See* Commerce Department/NSA Report, *supra* note 8.

111. *See International Market, supra* note 29.

112. *See* Telephone interview with Mr. Norman Zavala, CEI, Managua, Nicaragua (on file with the authors).

53. *Norfolk Island: Green*

Norfolk Island is a self-governing Australian territory located in the Tasman Sea east of Australia. It is offering Internet domain registration (".nf") free from government restrictions.

Norfolk Island is offering Internet domain names on a first come-first served basis. Norfolk Island is using the proceeds to fund a high-speed link to the Internet. The restriction-free aspect of Norfolk Island makes it another attractive cryptographic safe haven.[113]

54. *Norway: Green*

According to the Commerce/NSA Report, Norway's export controls are based on Royal Decree No. 967, Act No. 93 of December 18, 1987 relating to the control of the export of strategic goods, services, and technology, and Reg. No. 51 of January 10, 1989 relating to the implementation of the control of the export of strategic goods, services, and technology issued by the Ministry of Foreign Affairs.[114] The Ministry of Foreign Affairs, Section for Export and Import Controls, is the final authority for the approval or denial of export licenses.

There are no import controls in Norway. The Commerce/NSA report's section on domestic use prohibitions is totally redacted.[115] This may be a result of classified homologation procedures, instituted by the Norwegian PTT.

On July 8, 1997, Bendik Rugaas, the Norwegian Minister of National Planning and Coordination, Nils A. Rohne, the Norwegian Secretary of State for Trade and Industry, and Torstein Rudihagen, the Norwegian Secretary of State for Transport and Communications, endorsed the communiqué of the European Ministerial Conference on Global Information Networks in Bonn, Germany.[116]

55. *Pakistan: Red*

Pakistan prohibits the use of voice encryption technology.[117]

56. *Papua New Guinea: Green*

The Embassy of Papua New Guinea in Washington, D.C. informed EPIC that they were not aware of any laws in Papua New Guinea concerning cryptography. However, the Embassy of Papua New Guinea in-

113. *See Personal and Permanent Email Address & Norfolk Island Domain Names* (visited March 10, 1998) < http://www.names.nf>.

114. *See* Commerce Department/NSA Report, *supra* note 8.

115. *See* Commerce Department/NSA Report, *supra* note 8.

116. *See International Market*, *supra* note 29. The latest version of PGP (ver. 5.0) is available from the Norwegian web site at <http://www.ifi.uio.no/pgp>.

117. *See Crypto Law Survey*, *supra* note 7.

formed EPIC that jurisdiction for the technology was under the purview of the Department of the Attorney General of Papua New Guinea.[118]

57. *Philippines: Green*

The use of cryptography is not controlled by the Philippines.

58. *Poland: Green/Yellow*

The Embassy of Poland in Washington, D.C. informed EPIC that they had no information on the use of encryption in Poland. According to the Commerce/NSA Report, trade in encryption software is controlled as a military item by the Special Turnover Department of the Ministry of Foreign Economic Relations ("MFER").[119] The Special Turnover Department of the MFER issues special concessions in coordination with the Export Control Department of the MFER, which is responsible for dual-use commodities.

Encryption software is evaluated on a case-by-case basis. Poland acceded to the Wassenaar Arrangement in July 1996, thereby presumably agreeing to control the export of cryptography as a dual use (civilian-military) item.

On July 8, 1997, A. Zielinski, the Polish Minister of Telecommunications and Ms. M. Koslowska, the Polish Undersecretary of State for the State Committee for Scientific Research, endorsed the communiqué of the European Ministerial Conference on Global Information Networks in Bonn, Germany.[120]

59. *Portugal: Green/Yellow*

Portugal has acceded to the Wassenaar Arrangement and is presumably committed to restricting the export of cryptographic-enabled software as a dual-use item.

On July 8, 1997, Joao Cravinho, the Portuguese Minister for Infrastructure, M. Gago, the Portuguese Minister of Science and Technology, Dr. Leonor Coutinho, the Portuguese Secretary of State for Housing and Telecommunications, and Jose Penedos, the Portuguese Secretary of State for Industry and Economy, endorsed the communiqué of the European Ministerial Conference on Global Information Networks in Bonn,

118. *See* Letter from Embassy of Papua, New Guinea (Aug. 19, 1997) (on file with the authors).

119. *See* Commerce Department/NSA Report, *supra* note 8.

120. *See International Market, supra* note 29. *See also* Facsimile from Embassy of the Republic of Poland (July 18, 1997) (on file with the authors). PGP is available in Polish at <http://pipeta.chemia.pk.edu.pl/~kravietz/pgp>.

Germany.[121]

60. *Romania: Green / Yellow*

Romania has acceded to the Wassenaar Arrangement and is presumably committed to restricting the export of cryptographic-enabled software as a dual-use item.

On July 8, 1997, Sorin Pantis, the Romanian Minister of Communications, Eugen Constantin Isbasoiu, the Romanian Secretary of State for Education, Mircea Pusca, the Romanian Secretary of State for Research and Technology, Iustin Tanase, the Romanian Secretary of State for the National Commission for Informatics, and Sebastian Vladescu, the Romanian Secretary of State for Commerce and Industry, endorsed the communiqué of the European Ministerial Conference on Global Information Networks in Bonn, Germany.[122]

61. *Russia: Red*

According to the Commerce/NSA Report, upon the disintegration of the U.S.S.R., the President of Russia issued five decrees of February 22, March 27, April 11, May 12, and July 5, 1992 (Nos. 179, 312, 388, 469, and 507), which, together with the Law on Defense Industry Conversion, specified certain legal foundations for a national armaments and military technologies control system.[123] These decrees were consolidated in 1994 by the "Statute on Controls of Exports from the Russian Federation of Certain Types of Raw and Processed Materials, Equipment, Technology, Scientific and Technical Information Which Can Be Used in the Production of Weapons or Military Equipment" as ratified by the President of the Russian Federation under Decree No. 74 of February 11, 1994. Included in this statute is a list of commodities, which require an individually approved license, issued by the Ministry of Foreign Economic Relations for export from Russia. Cryptographic equipment and software (including mass-market) is identified in the list of commodities requiring individually approved export licenses.

Section 5 of Edict No. 334, of April 3, 1995, issued by the President of Russia prohibits the import of cryptographic products without a license. Section 4 of Edict No. 334, of April 3, 1995, issued by the President of Russia prohibits all activities in the development, sale, and use of cryptography without a license issued by the Federal Agency for Government Communications and Information ("FAPSI"), Russia's equivalent of

121. PGP is available in Portuguese at <http://eunice.dei.uc.pt/pgp>. *See also International Market, supra* note 29.

122. *Id.*

123. *See* Commerce Department/NSA Report, *supra* note 8.

the NSA.[124]

62. *Saudi Arabia: Green*

According to the NIST Survey, Saudi Arabia has no import or export controls on cryptography.[125]

63. *Singapore: Red*

> According to the Singapore Trade Development Board:
> The import of scrambler, or encryption hardware or software capable of re-arranging signs, signals, writing, sounds, or intelligence for the purpose of secrecy is controlled by the Trade Development Board ("TBD") under the First Schedule of the Regulation of Imports and Exports Regulations 1995.
> Prior written approval from the TDB must be obtained before the import is allowed into Singapore. To apply for the import approval, an importer is required to complete the 'Application to Import Encryption Hardware/Software' and submit it to the TDB for consideration. TDB requires the importer to furnish the technical specifications of the encryptor and to provide the end-user's justification for the use of the encryptor. The importer must be a company incorporated or registered in Singapore.
> TDB will notify the importer in writing of the outcome of his Application. If the importer is allowed, the importer should also apply for a license from the Telecommunications Authority of Singapore ("TAS"), Licensing Department, to use the encryptor (for hardware only).[126]

This information was contained in a letter from Ms. Ruby Goh, Trade Officer of the Imports and Exports Office. No mention was made of export controls. Therefore, it is a strong probability that there are no export controls in place in Singapore.

Similarly, no mention was made of domestic use controls, although the rigidity of the import controls indicate that domestic freedom of use may be restricted.[127]

64. *Slovakia: Green / Yellow*

The Commercial and Economic Section of the Embassy of Slovakia in New York, New York informed EPIC that they had no information on encryption laws being enacted in Slovakia. However, they referred EPIC

---

124. *See International Market, supra* note 29.

125. *See* NIST Survey, *supra* note 6.

126. Letter from Ms. Ruby Goh, Trade Officer of the Imports and Exports Office, Singapore (March 1995) (on file with the authors).

127. *See* Facsimile from Singapore Trade Development Board, Singapore (Aug. 11, 1997) (on file with the authors).

to the Foreign Commercial Service of the United States Embassy in Bratislava, Slovakia for information on Slovak laws.

The role of the American Embassy most likely reflects Slovakia's adherence to the post-COCOM Wassenaar Arrangement, to which Slovakia acceded in July 1996. The Wassenaar Arrangement establishes controls on the export of dual military and civilian use goods. Cryptographic-enabled software is deemed a dual-use item.

On July 8, 1997, Jan Jasovsky, the Slovak Minister of Transport, Posts, and Telecommunications, endorsed the communiqué of the European Ministerial Conference on Global Information Networks in Bonn, Germany.[128]

65. *Slovenia: Green*

EPIC's letter to the Slovenian Embassy was not answered.[129] On July 8, 1997, Lojze Marincek, the Slovenian Minister of Science and Technology and Miro Rozman, endorsed the communiqué of the European Ministerial Conference on Global Information Networks in Bonn, Germany.[130]

66. *South Africa: Yellow*

According to the Commerce/NSA Report, the South African government controls encryption as a dual-use item on the General Armaments Control Schedule.[131] Exports of encryption require an individual validated license. The control of encryption is under the jurisdiction of the South African Department of Defense Armaments Development and Protection Act, 1968, No. R. 888, published on May 13, 1994.

An individual validated license is required for the import of encryption software. A valid permit from the Armaments Control Division is required for the import or transportation of cryptographic equipment or software.[132]

67. *Spain: Yellow*

According to the Directorate General of Telecommunications in Madrid, Spain utilizes administrative and legal measures to implement the

128. Facsimile from Embassy of the Slovak Republic, Commercial and Economic Section, New York (July 25, 1997) (on file with the authors).

129. However, PGP is available in Slovenian at <http://www.e5.ijs.si/security/wwwpks/pks-toplev.html>.

130. *See International Market, supra* note 29.

131. *See* Commerce Department/NSA Report, *supra* note 8.

132. *See International Market, supra* note 29; *see also* United States Embassy State Department Johannesburg Cable 000951, Johannesburg, South Africa (June 23, 1995) (on file with the authors).

European Union Council Resolution of January 17, 1995 on the lawful interception of telecommunications, 9529/95 ENFPOL. Currently, there are no specific laws in Spain on encryption policy.

In every telecommunications service regulation, service providers are reminded of their obligation to decrypt intercepted communications for the legal authorities under Art. 579 of the Law on Criminal Investigations. The government agency responsible for cryptography export and import controls is the Directorate General for Foreign Commerce (within the Ministry of Economics). The department responsible for regulating the domestic use of encryption is the Directorate General of Telecommunications (within the Ministry of Planning).

According to the Commerce/NSA Report, Spain adopted export regulations conforming to COCOM on May 28, 1993.[133] Spain later acceded to the Wassenaar Arrangement in 1995. The Spanish law is codified in Royal Decree 824 of September 21, 1993 and its annexes. The legislation establishes an inter-governmental committee to review export license applications as well as establish necessary policies in this area. The committee, the *Junta Interministerial Reguladora del Comercio de Material de Defensa y Doble Uso* ("JIMDDU"), is presided over by the Secretary General for Commerce and includes representatives of the Defense Directorates and Foreign Affairs and Economic Ministries. Licenses are approved or denied on an individual basis dependent upon the effects on Spanish foreign policy or national defense as well as international commitments.

Most exports from Spain require an individually validated license for all destinations, although the law makes provision for general licenses and distribution licenses. Security products containing confidentiality features require individual licensing, even for European Union and the Wassenaar Arrangement member nations. Exceptions may be granted for mass-market software products.

The formulation of national cryptographic policies for Spain is under the authority of the Director General of the *Centro Superior de Informacion de la Defensa* ("CESID"), the Spanish intelligence service that comes under the control of the Ministry of Defense.

Additionally, Import authorizations are addressed by Royal Decree 824 of September 21, 1993, and licenses are required for articles listed in Annex 6. Cryptographic products are exempt from licensing although Spain will supply import certificates for cryptographic products if required by the exporting country for delivery certification.

Although no Spanish law specifically regulates the public use of cryptography, a State Department Madrid Cable 120521Z, August 1994, states that, based upon discussions with Public Works officials, "[t]he

133. *See* Commerce Department/NSA Report, *supra* note 8.

Ministries of Interior, Public Works, and Trade are the key regulators of the private use of encryption. Outside of government agencies and law enforcement and bank data transfer networks, the use of private encryption is not currently authorized."[134] This is at variance with the Planning Ministry's contention that telecommunications providers are obligated provide decrypted communications to legal authorities.

On July 8, 1997 Josep Pique I Camps, the Spanish Minister of Industry and Energy, endorsed the communiqué of the European Ministerial Conference on Global Information Networks in Bonn, Germany.[135]

68. *Swaziland: Green*

According to the Embassy of Swaziland in Washington, D.C., the country does not have policies on the importation, exportation, or domestic uses of cryptographic hardware or software.[136]

69. *Sweden: Green*

According to the Embassy of Sweden in Washington, D.C., there are in Sweden:

1.) No controls on the domestic use of cryptography.
2.) No controls on the import of computer programs or equipment that permit cryptography.
3.) Controls on the export of domestically developed computer programs or equipment that permit cryptography. These goods require an export license. The governing act is the Strategic Products Act of 1991 (Swedish Code of Statutes 1991:341; Amendments 1995:1661)
4.) The agency that is responsible for policy matters on cryptography is the Division of European Integration/Strategic Export Control ("EI/ESEK"). This agency resides within the Ministry of Foreign Affairs. At present, a study group comprising people from several Swedish ministries is working on a new cryptography policy. The study group is led by Ambassador Magnus Faxen.

The Commerce/NSA Report concurs that there are no import or domestic user restrictions in Sweden.[137] On July 8, 1997 Peter Nygards,

134. *See* United States Embassy State Department Madrid Cable 120521Z, Madrid, Spain (August 1994) (on file with the authors).

135. *See International Market, supra* note 29; *see also* Facsimile from Ministry of Planning, Madrid (July 21, 1997) (on file with the authors). PGP is available in Catalan at <http://diable.upc.es/~marcos/pgp.html>.

136. *See* Letter from Embassy of the Kingdom of Swaziland (Aug. 6, 1997) (on file with the authors).

137. *See* Commerce Department/NSA Report, *supra* note 8.

the Swedish Secretary of State for Industry and Trade, endorsed the communiqué of the European Ministerial Conference on Global Information Networks in Bonn, Germany.[138]

70. *Switzerland: Green*

The Embassy of Switzerland in Washington, D.C. responded in quite some detail on its cryptographic policies:

1.) Controls on the use of encryption software or hardware:
   a.) According to the Federal Law on Telecommunications (*Loi fédérale du 21 juin 1991 sur les télécommunications*, RS 784.10) and its implementing ordinances:
      1.) The production of cryptographic software and hardware is not subject to any limitation.
      2.) The use of cryptographic software is not subject to any limitation.
      3.) Cryptographic products as well as other telecommunications equipment that can be connected with a public telecommunications network must be approved by the Federal Office of Communications ("FOC").
      4.) Radio communications must normally occur in plain text, a license permitting encryption may, nevertheless, be obtained from the FOC. For other forms of telecommunications, encryption is permitted without a license.
2.) Controls on the import of encryption:
   a.) The ordinance concerning the export of transit of products does not stipulate any licensing obligation for the import of products, including cryptographic hardware and software.
   b.) The only rules applicable in this context are those relating to the Import Certificate ("IC"). The IC is one of the documents that may be necessary for the supplier to obtain an export license from the authorities in the country of origin. It is, therefore, up to the authorities of the country of origin to determine whether or not an IC is to be required from the country of destination in order to get a license.
   c.) For imports of cryptographic equipment, Switzerland issues an IC only if there is a formal request from the country of origin.
   d.) As for exports of cryptographic equipment, Switzerland normally requires the presentation of an IC from all the countries of destination, the authorities of which issue such a document. Member countries of all the four international export control regimes are exempted from this requirement: The Australia Group ("AG"), the Missile Technology Control Regime ("MTCR"), the Nuclear Supplier's Group ("NSG"), and the Wassenaar Arrangement ("WA").

138. *See International Market, supra* note 29; *see also* Letter from Embassy of Sweden (July 22, 1997) (on file with the authors).

3.) Export controls on encryption:
   a.) Encryption equipment, software, and technology are controlled under the Ordinance concerning the export and transit of products (*Ordonnance du 22 décembre 1993 sur l'exportation et le transit de produits*; RS 946. 221; RO 1994 426; 1995 5651) and its annex (Part I / Munitions List, ML 11 & Part III / Industrial List, Category 5, Part 2 – Information Security). This annex corresponds to the International Munitions List ("International Atomic Energy List") and International Industrial List that were agreed upon by the participating countries to the negotiation of the Wassenaar Arrangement ("WA") on March 31, 1994. The present Control Lists ("IL & ML") of the WA will be implemented in Switzerland together with a new law on the control of dual use goods, presumably before the end of 1997.
   b.) The export and re-export of cryptographic hardware, software, and technology listed in the aforementioned ordinance requires an individual validated license. However, deliveries to end-users in the countries that are members of all the four international export control regimes (i.e., AG, MTCR, NSG, and WA) are exempted from the license obligation.
   c.) The Swiss Federal Office of Foreign Economic Affairs ("FOFEA") is the licensing agency. The specific criteria considered in determining whether to grant a license are those of the WA, namely "to prevent the acquisition of armaments and sensitive dual-use items for military end-uses, if the situation in a region or the behavior of a state is, or becomes, a serious concern for the participating states."
   d.) The transit is subject to a limited prohibition. If the country of origin restricts the export of the products listed in the annex (e.g., cryptographic products), their transit is forbidden if it cannot be proven (e.g., with a license) that the transfer to the new country of destination is in accordance with the legislation of the country of origin.
4.) Export controls are overseen by the Swiss Federal Office of Foreign Economic Affairs ("FOFEA"). Restrictions on the domestic use of cryptography on public telecommunications networks are the responsibility of the Federal Office of Communications ("FOC"):
   a.) The Commerce/NSA Report concurs that there are no import or domestic use restrictions in Switzerland.[139]

On July 8, 1997 Franz Blankart of the Swiss FOFEA, endorsed the communiqué of the European Ministerial Conference on Global Information Networks in Bonn, Germany.[140]

139. *See* Letter from the Embassy of Switzerland (June 31, 1997) (on file with the authors).

140. *See International Market, supra* note 29; *see also* Letter from the Embassy of Switzerland, *supra* note 91.

71. *Taiwan: Yellow*

EPIC was informed by the Economic Division of the Taipei Economic and Cultural representative Office in Washington, D.C. that the Republic of China's Research, Development, and Evaluation Commission of the Executive Yuan had prepared a "Report on the Establishment of a Public Key Infrastructure" ("PKI") in Taiwan.[141] The PKI initiative calls for the setting up of a root Certificate Authority ("CA") and the development of national "trust chains."[142] The government's proposal states that "any private or public organization that wishes to act as a CA may do so only after applying for and receiving a license from the designated [government] agency."[143] The responsible agencies are indicated as the Research, Development, and Evaluation Commission of the Executive Yuan, the Ministry of Economic Affairs, and the Ministry of Justice.[144] The proposal also states that "[a]fter taking into consideration the needs of national security, economic development, law enforcement, and personal privacy, a feasible 'key escrow and recovery' scheme should be devised on the basis of experience gained in Europe and America."[145] The proposal also recommends that "to meet the needs of universal electronic commerce and electronic government, a 'national electronic signature authentication system' should be implemented in coordination with the issuance of personal identification cards containing embedded IC [integrated circuit] chips."[146]

According to the Commerce/NSA Report, Taiwan is an active importer of encryption software, with the United States claiming fifty-six percent of the market.[147] There are no reported domestic use restrictions, however, Taiwan is a party to the Wassenaar Arrangement and is committed to restricting the export of cryptographic products.[148]

72. *Tibet: Green*

According to the Office of Tibet in London, England, the Government-in-exile currently does not use cryptography and has no policies in

141. *See* Republic of China's Research, Development, and Evaluation Commission of the Executive Yuan, Report of the Establishment of a Key Infrastructure (on file with the authors).

142. *See id.*

143. *See id.*

144. *See id.*

145. *See id.*

146. *See id.*

147. *See* Commerce Department/NSA Report, *supra* note 8.

148. *See International Market*, *supra* note 29; *see also* Letter from Taipei Economic and Cultural Representative Office, Washington, D.C. (Sept. 23, 1997) (on file with the authors). PGP in Chinese is available from Taiwan via the Internet at <http:// pgp.tnjc.edu.tw/cpgp. html>.

place on its use.[149]

73. *Turkey: Yellow*

Turkey has acceded to the Wassenaar Arrangement and is presumably committed to restricting the export of cryptographic-enabled software as a dual-use item.

74. *Ukraine: Yellow*

Ukraine has acceded to the Wassenaar Arrangement and is presumably committed to restricting the export of cryptographic-enabled software as a dual-use item.

75. *United Kingdom: Green / Yellow*

According to the Commerce/NSA Report, the United Kingdom export controls of cryptographic products are detailed in Export of Goods Control Orders ("EGCO"), the latest version of which is dated April 24, 1994.[150] These statutory instruments derive their authority from the Import, Export, and Customs Defence Act of 1939. The EGCO stipulates that no form of information security material, technology, or technique may be exported without an export license. The order makes no distinction between products designated for "government-classified" or "commercial" encryption purposes and makes no specific reference to the Data Encryption Standard ("DES") or any other algorithm. It reflects the details of COCOM lists, and subsequently, the Wassenaar Arrangement amendments.

According to the Department of Trade and Industry ("DTI"):

> an export license may be obtained by applying to the DTI. In practice, however, [United Kingdom] vendors of these goods also send a [facsimile] of their applications to the Communications and Electronics Security Group ("CESG"), simultaneously with the transmittal of the application to DTI so as to speed up the decision process. CESG is part of GCHQ, the [United Kingdom's] NSA equivalent, but has a separate identity to facilitate work with unclassified commercial entities. CESG reviews the application and (on paper) advises DTI of its view. In practice, DTI generally follows the CESG recommendation and does not approve the export item that CESG finds unacceptable.[151]

According to Department of Trade and Industries' Export Control Organization Notice STU/1,[152] the United Kingdom has sanctions and

149. *See* Letter from Office of Tibet (July 1, 1997) (on file with the authors).

150. *See* Commerce Department/NSA Report, *supra* note 8.

151. *See* Department of Trade and Industries' Export Control Organization Notice, STU/9/3/2, Issue 14, Nov. 1996.

152. *See id.*

partial or total embargoes in place against Angola, Iraq, Libya, Argentina, Armenia, Azerbaijan, Bosnia and Herzegovina, China, Croatia, Iran, Liberia, Montenegro, Myanmar (Burma), Nigeria, Rwanda, Serbia, Somalia, Taiwan, the states of former Yugoslavia, and Congo (Kinshasa).

There are no import controls on cryptologic products in the United Kingdom. There do not appear to be any domestic use restrictions. The United Kingdom began a Public Consultation on the regulation of Trusted Third Parties ("TTPs") for the provision of encryption services. This resulted in the release of the DTI Public Consultation Paper on detailed proposals for legislation on the Licensing of TTPs for the provision of encryption service. The election of a new Labour Party government has resulted in a moratorium on the proposed legislation with strong indications that the Labour Party may stand by its campaign pledge of not introducing any controls on the use of encryption in the United Kingdom. The Labour Parties' stand on cryptography is spelled out as follows:

> It is important that privacy is rigorously protected over the new networks, for both personal and commercial reasons. We do not accept the "clipper chip" argument developed in the United States for the authorities to be able to swoop down on any encrypted message at will and unscramble it.
>
> The only power we would wish to give to the authorities, in order to pursue a defined legitimate anti-criminal purpose, would be to enable decryption to be demanded under judicial warrant (in the same way that a warrant is required in order to search someone's home).
>
> Attempts to control the use of encryption technology are wrong in principle, unworkable in practice, and damaging to the long-term economic value of the information networks. There is no fundamental difference between an encrypted file and a locked safe. A safe may be effectively impregnable in that the effort taken to open it would destroy the contents. An encryption algorithm, similarly, may be effectively unbreakable.
>
> Furthermore, the rate of change of technology and the ease with which ideas or computer software can be disseminated over the Internet and other networks make technical solutions unworkable. Adequate controls can be put in place based around current laws covering search and seizure and the disclosure of information. It is not necessary to criminalize a large section of the network-using public to control the activities of a very small minority of law-breakers.[153]

On July 8, 1997 John Battle the British Minister for Science, Energy and Industry, endorsed the communiqué of the European Ministerial Conference on Global Information Networks in Bonn, Germany.[154]

153. *See New Labour New Britain* (visited March 2, 1998) <http://www.labour.org.uk/views/info-highway/content.html>.

154. *See International Market, supra* note 29.

76. *United States: Yellow / Red*

In February 1996, the International Traffic in Arms Regulations ("ITAR") was amended to permit the temporary export of personal use encryption software. Licenses were waived in these cases, provided the user adequately provided security for the encryption software while traveling overseas.

In 1996, the International Traffic in Arms Regulation governing the export of cryptography was overhauled. Responsibility for cryptography exports was transferred to the Department of Commerce from the Department of State. However, the Department of Justice is now part of the export review process. In addition, the National Security Agency ("NSA") remains the final arbiter of whether to grant encryption products export licenses and it has staff assigned to the Commerce Department and many other federal agencies that work with encryption policy and standards, including the State Department, Justice Department, National Institute for Standards and Technology ("NIST"), and the Federal Communications Commission. Cryptography that embeds key recovery mechanisms receives favorable treatment in the decision-making process.

Export licenses are considered for different categories of encryption items. The encryption items are differentiated in five categotries.

1. Mass-market encryption software may be freely exported after a one-time review.
2. "Key recovery" cryptographic products are eligible for an export license to non-embargoed countries.
3. 56-bit cryptography can be granted a six-month export license after a one-time review, provided the exporting vendor commits to incorporating key recovery features within two years. After two years, the export of non-key recovery 56-bit cryptography will be once again prohibited again.
4. Other encryption items may receive export licenses on a case-by-case basis.
5. Encryption "technology" may be licensed for export on a case-by-case basis.

There are no import restrictions on cryptography. There are no domestic use controls on cryptography. However, on September 3, 1997, Federal Bureau of Investigation ("FBI") Director Louis Freeh called for Congressional passage of the Secure Public Networks Act,[155] which would require all United States encryption products to have a backdoor for law enforcement and other government access. Freeh stated that "mandatory key recovery, to the extent that it was implemented, would

155. H.R. 695, 105th Cong. (1997).

be the best law enforcement solution" for the administration. The FBI sponsored legislation would require all manufacturers of encryption products and network services to include key recovery or escrow mechanisms that would that would provide the government with "immediate decryption of communications or electronic information encrypted by such products or services on the public network." The FBI-supported legislation would also empower the Attorney General to act as final arbiter of whether an encryption method conforms to government eavesdropping standards. No new technology with encryption mechanisms would be able to be manufactured, sold, resold, distributed, or imported without the prior approval of the chief law enforcement official of the United States.

In California, Senate Bill 1133 was introduced on February 28, 1997.[156] California Senate Bill 1133 cautions the Federal government against adopting a mandatory key recovery system. Specifically, California Senate Bill 1133 states:

> The key recovery period will not solve government of industry's needs. The administration's current policy will not solve the concerns of law enforcement and national security, and there is little or no market demand for key recovery cryptography ("KRC") for electronic communications. Without a comprehensive multilateral agreement prohibiting the sale of non-KRC, law enforcement targets will have access to non-KRC from foreign sources. Customers prefer non-KRC and are unlikely to use key recovery products when they can buy non-KRC. The administration's current policy would deny United States companies the ability to offer competitive products to the world market; this will adversely affect jobs and the economy.[157]

B. The Organization for Economic Cooperation and Development: ("OECD") Guidelines on Cryptography Policy

The Organization for Economic Cooperation and Development ("OECD") issued Guidelines on Cryptography Policy on March 27, 1997. Similar to the Walsh Report in Australia and the Danish IT Security Council policy, the Guidelines failed to endorse a United States sponsored initiative for the OECD to support an international key escrow recovery framework.

The OECD Recommendation is a non-binding agreement that identifies the basic issues that countries should consider in drawing up cryptography policies at the national and international level. The

156. S. 1133, 1997-98 Leg., Reg. Sess. (Cal. 1997).

157. *Id.*

Recommendation culminates one year of intensive talks to draft the Guidelines.

The OECD Guidelines state:

> The need for Guidelines emerged from the explosive worldwide growth of information and communications networks and technologies and the requirement for effective protection of the data which is transmitted and stored on those systems. Cryptography is a fundamental tool in a comprehensive data security system. Cryptography can also ensure confidentiality and integrity of data and provide mechanisms for authentication and non-repudiation for use in electronic commerce.
>
> Governments want to encourage the use of cryptography for its data protection benefits and commercial applications, but they are challenged to draft cryptography policies which balance the various interest at stake, including privacy, law enforcement, national security, technology development and commerce. International consultation and co-operation must drive cryptography policy because of the inherently international nature of information and communications networks and the difficulties of defining and enforcing jurisdictional boundaries in the new global environment.
>
> The Guidelines are intended to promote the use of cryptography, to develop electronic commerce through a variety of commercial applications, to bolster user confidence in networks, and to provide for data security and privacy protection.
>
> Some OECD Member countries have already implemented policies and laws on cryptography, and many countries are still developing them. Failure to co-ordinate these national policies at the international level could introduce obstacles to the evolution of national and global information and communications networks and could impede international trade. OECD governments have recognized the importance of international co-operation, and the OECD has contributed by developing consensus on specific policy and regulatory issues related to cryptography and, more broadly, to information and communications networks and technologies.[158]

The Guidelines set out eight basic Principles for cryptography policy:

1.) Cryptographic methods should be trustworthy in order to generate confidence in the use of information and communications systems.

2.) Users should have a right to choose any cryptographic method, subject to applicable law.

3.) Cryptographic methods should be developed in response to the needs, demands and responsibilities of individuals, businesses and governments.

158. *See* The Organization for Economic Cooperation and Development: ("OECD") Guidelines on Cryptography Policy (on file with the authors).

4.) Technical standards, criteria and protocols for cryptographic methods should be developed and promulgated at the national and international level.
5.) The fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods.
6.) National cryptography policies may allow lawful access to plain text, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible.
7.) Whether established by contract or legislation, the liability of individuals and entities that offer cryptographic services or hold or access cryptographic keys should be clearly stated.
8.) Governments should co-operate to co-ordinate cryptography policies. As part of this effort, governments should remove, or avoid creating in the name of cryptography policy, unjustified obstacles to trade.[159]

C. Council of Europe

On September 8, 1995, the Council of Europe approved a recommendation to ban strong cryptography in their member states. The Council is not like the European Commission in that it has no statutory authority to enforce its recommendations. However it is rare for member countries to reject Council of Europe's recommendations. The proposal, Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information Technology (Adopted by the Committee of Ministers on September 11, 1995), makes telecommunications service providers responsible for decrypting traffic and supplying it to governments when required. Specifically the proposal states:

> Subject to legal privileges or protection, investigating authorities should have the power to order persons who have data in a computer system under their control to provide all necessary information to enable access to a computer system and the data therein. Criminal procedure law should ensure that a similar order can be given to other persons who have knowledge about the functioning of the computer system or measures applied to secure the data therein.
> Specific obligations should be imposed on operators of public and private networks that offer telecommunications services to the public to avail themselves of all necessary technical measures that enable the interception of telecommunications by the investigating authorities.

159. *See id.*

Specific obligations should be imposed on service providers who offer telecommunications services to the public, either through public or private networks, to provide information to identify the user, when so ordered by the competent investigating authority.
Measures should be considered to minimize the negative effects of the use of cryptography on the investigation of criminal offenses, without affecting its legitimate use more than is strictly necessary.[160]

VII. CONCLUSION OF THE SURVEY

Few countries today have controls in place that restrict the use of cryptography. Many countries, large and small, industrialized and developing, seem to be ambivalent about the need to control encryption technology. For many countries, cryptography policy is not a significant national issue. For those that have considered the topics, interests in electronic commerce and privacy appear to outweigh the concerns expressed by law enforcement.

Some major United States allies oppose the United States attempt to export its concept of key recovery. The United States has tried to enlist the support of Brazil, Singapore, South Africa, Brunei, Indonesia, Vietnam, and Malaysia to support its international key recovery proposals. There has also been a smaller-scale effort by the United States to win the support of other developing countries in Latin America, Africa, Asia, and the Pacific. All of the former countries were contacted in EPIC's survey, however, only a few responded. It is doubtful, based upon the results of EPIC's survey, that the United States is achieving much in the way of success *vis à vis* the developing nations.[161]

---

160. *See Recommendation Concerning Problems of Criminal Procedure Law Connected with Information Technology* (visited on March 5, 1998) <http://www.privacy.org/pi/intl_orgs/coe/info_tech_1995.html>.

161. In a January 28, 1997 speech to the RSA Data Security Conference in San Francisco, U.S. special ambassador for cryptography, David Aaron, stated that U.S. allies "support the concept of lawful access by governments" to encrypted files and communications and that "many governments in the interest of public safety, want stronger controls than we have." *Id.* The envoy made some specific points about what all governments in the world want with regard to cryptography:

1.) All governments recognize the need for international cooperation to create a KMI (Key Management Infrastructure) and certificate services to facilitate privacy and electronic commerce;
2.) All support the concept of lawful access by governments and the use of trusted parties and/or key escrow as a possible mechanism;
3.) Many governments, in the interest of public safety, want stronger controls than we have. They have, or are considering, domestic controls on the use of encryption within their borders;
4.) Virtually every government has expressed unhappiness with the US decision to release 56 bit non-key recovery products even with key recovery commitments. Several have criticized the absence of internal US controls; and

EPIC also concluded that many national intelligence and law enforcement agencies seem to have "hijacked" the cryptography issue for their own benefits, and in many cases leaving foreign affairs and trade ministries unaware of what policies governments are following. EPIC's responses from some embassies in Washington, D.C. including those of large countries like Australia, support this argument. The July 1997 Bonn Ministerial meeting, which endorsed the OECD Cryptography Guidelines and stressed the need for privacy, was heavily attended by trade and science ministers. However, the German Justice Minister and the Cypriot Interior Minister even endorsed the final communiqué of the meeting.

The unrestricted use of techniques to protect personal privacy, such as encryption, remains an important concern for the international civil liberties and human rights communities. It should be anticipated that efforts by national governments to restrict the use of this technology will be opposed by these organizations.

There appears to be an awareness gap between those electronic privacy and major human rights groups that are concerned about cryptography and their counterparts in developing nations that have not been sufficiently informed on the subject. It is necessary to launch an education campaign to inform various political, labor, social, ethnic and minority rights, religious, humanitarian assistance, and other groups on the benefits and techniques of using cryptography. This is especially important as such groups continue to rely more on the Internet for communications and public education.

Attempts by the United States to influence the development of restrictive national and international regimes on the use of cryptography should be raised as a political and civil rights issue by sympathetic political parties and organizations. While our survey indicates a general ambivalence by a majority of the world's nations on the unrestricted use of cryptography, there is reason to believe that this situation could significantly change. The combined and formidable resources of American and other law enforcement and intelligence agencies as well as international

---

5.) They are concerned that the increased availability of such products without key recovery could undermine their ability to protect the public safety within their borders.

Id. The EPIC survey contradicts all the aforementioned points. We discovered that not only is there confusion about if, or how, to address cryptography use among nations, but there appears to be a great deal of confusion within governments on what, if any, policies to pursue. Moreover, a large number of countries failed to respond to EPIC's survey, indicating either a lack of understanding of the issue or a lack of concern on their part. Countries staking their future on the ability to access the Internet for electronic commerce noticeably did not respond to EPIC's survey. These include Bangladesh, Barbados, Bermuda, Chile, Egypt, Ghana, Jamaica, Malaysia, Mauritius, New Zealand, Saint Lucia, Sri Lanka, Thailand, Trinidad and Tobago, and Venezuela. *Id.*

structures like Interpol and the G-8, could be successful in forcing the world to adopt an international encryption key management infrastructure. Our major goal must be to prevent such an occurrence.