Steptoe & Johnson's E-Commerce Practice Group

Overview

Encryption regulatory issues have been, and will continue to be, a hazardous area for companies attempting to comply with country regulations. Steptoe & Johnson LLP'S electronic commerce practice offers a unique service to clients seeking information on the regulation of cryptography around the world. We have an international team of lawyers based in both Europe and the United States, whose combined experience spans decades.

As well as being advisory leaders in encryption issues**,** Steptoe has also developed a broad network of information sources including regulatory bodies throughout the world such as OECD, local embassies and government agencies, commercial networks and organisations. These contacts give the practice group the unique ability to send quick inquiries to encryption policymakers in numerous countries, and to obtain informal guidance about cryptography policy in those countries. Our contacts are particularly useful in countries that do not publish the details of their encryption policies. Steptoe regularly deal with private-sector individuals and companies that have hands-on experience with encryption regulations from around the world. In addition, we are experienced in dealing with country-specific encryption export and import licensing proceedings.

It is Steptoe's goal to supply concise, accurate descriptions of the relevant laws and regulations on export, import and use of encryption in a large number of countries. We provide this content in a convenient, searchable, Web-based format. Furthermore, in producing this content, we have developed a broad network of government and private contacts in the countries on which we report. These contacts can provide a valuable resource for companies who have particularly difficult questions requiring special attention.

In summary, we believe that the information we provide is a valuable and cost-effective resource for companies that wish to ensure compliance with international encryption regulations. In addition to the Steptoe Country-by-Country Guide to Encryption, this guide also explains the value of understanding international encryption regulation and introduces the key resources in our electronic commerce team.

Steptoe & Johnson LLP
1330 Connecticut Avenue, NW
Washington, DC 20036
Tel: 202.429.3000
Fax: 202.429.3902

750 Seventh Avenue
Suite 1900
New York, NY 10019
Tel: 212.506.3900
Fax: 212.506.3950

115 South LaSalle Street
Suite 3100
Chicago, IL 60603
Tel: 312.577.1300
Fax: 312.577.1370

Collier Center
201 East Washington Street,
16th Floor
Phoenix, AZ 85004
Tel: 602.257.5200
Fax: 602.257.5299

633 West Fifth Street
Suite 700
Los Angeles, CA 90071
Tel: 213.439.9400
Fax: 213.439.9599

2121 Avenue of the Stars
Suite 2800
Los Angeles, CA 90067
Tel: 310.734.3200
Fax: 310.734.3300

Avenue Louise 240, Box 5
B-1050 Brussels
Belgium
Tel: +32 2 626 0500
Fax: +32 2 626 0510

Steptoe & Johnson
99 Gresham Street
London, EC2V 7NG
England
Tel: +44 (0)20 7367 8000
Fax: +44 (0)20 7367 8001

Steptoe & Johnson's E-Commerce Practice Group

Steptoe & Johnson's Electronic Commerce Practice Group represents leading financial services, information services, hardware and software firms on the wide array of issues that arise when a new digital product or service is introduced, as well as on liability issues and interaction with law enforcement agencies. We advise technology companies on liability and other legal consequences arising from the use of digital signatures and certificates for electronic commerce. We have extensive legal and technical experience in data encryption technology, the application of which is considered essential to conducting reliable and secure electronic commerce.

Tom Barba is a partner in the Technology Department at Steptoe's Washington, DC office. Tom combines 25 years of civil litigation experience with decades of expertise advising technology companies on public policy issues. Tom has advised telecommunications carriers and equipment manufacturers wiretap compliance and conducted related litigation since before the passage of CALEA. At the Justice Department in the late 1980s, Tom served as Deputy Assistant Attorney General for the Civil Division and, among many various responsibilities, defended the FBI and the Organized Crime and Racketeering Section of the Criminal Division in cases involving title III wiretaps. Tom has represented AT&T and AT&T Wireless in CALEA matters and in the Radio Frequency Multi District Litigation Case and on other telecommunications policy questions. He also spent several years analyzing, negotiating and implementing the international wiretapping capabilities of one of the first worldwide satellite telecommunications networks.

Maury Shenk is a partner in Steptoe's London office and is a dual-qualified US/UK lawyer. Mr. Shenk manages Steptoe's European technology practice, and focuses on the international aspects of telecommunications and electronic commerce. He advises clients on the legal aspects of conducting business online, including issues of data protection, jurisdiction, intellectual property, competition and liability in the online environment, as well as commercial agreements, acquisitions and other transactions. Mr. Shenk supervises Steptoe & Johnson's leading encryption export/import practice.

Michael Vatis is a partner at Steptoe's New York office. His practice focuses on Internet, e- commerce, and technology matters, with special emphasis on issues involving security, intelligence, and law enforcement. He was the founding director of the National Infrastructure Protection Center at the FBI, the first government organization responsible for detecting, warning of, and responding to cyber attacks, including computer crimes, cyber terrorism, cyber espionage, and information warfare. Mr. Vatis has regularly testified before congressional committees on counterterrorism, intelligence, and cyber security issues. He is also interviewed on television, radio, and in print media, and has been a guest lecturer at law schools and universities and a frequent speaker at industry conferences worldwide.

Steptoe & Johnson's E-Commerce Practice Group

Daniel C. H. Mah is an associate in the Washington office of Steptoe & Johnson. Mr. Mah focuses primarily on telecommunications and electronic commerce. He has worked on several major telecommunications mergers before the Federal Communications Commission (FCC) and the US Department of Justice. He has also represented clients on various satellite licensing and copyright issues, the wiretap and CALEA responsibilities of carriers, the regulation of Voice over Internet Protocol, data privacy, and the disclosure responsibilities of financial institutions. In 2002, Mr. Mah completed a doctoral thesis at Stanford Law School, entitled "A Tale of Two Networks: Interconnection in Early Telephony and the Internet." While his inquiry focused on network interconnection strategy and policy, his research spanned such related topics as telecommunications history, the privatization of the Internet, Internet peering agreements, and cable open access.

Sally Albertazzie is a specialist in Steptoe's eCommerce practice group. She is a graduate of Georgetown University's Paralegal Institute and has over 10 years experience in all aspects of technology. Ms. Albertazzie coordinates workflow, publishes our weekly newsletter, E-Commerce Law Week, handles much of the research needed by group attorneys, and supervises the group's paralegals.

The team has represented numerous companies providing encryption and electronic payment services on regulatory, legislative and corporate contractual matters. As well as advising credit card associations and issuers on the use of cryptography for commercial applications, the team has also advised numerous firms on electronic commerce data protection, consumer protection, and privacy initiatives in the United States, European Union and other jurisdictions.

Globally recognised clients include:

- Internet service providers, including the world's largest
- Numerous software companies
- Two of the top global credit card associations
- Global investment banks
- One of the worlds largest petroleum companies
- Other global technology companies

Steptoe & Johnson's E-Commerce Practice Group

The Value of Understanding International Encryption Regulation
Encryption technology offers both substantial benefits (by protecting the security, authenticity and integrity of business and personal communications) and substantial risks (by making it easier for criminals and terrorists to conceal communications regarding illegal behaviour). While most countries recognize the benefits of encryption, the associated risks have led many governments to impose controls on import and export of encryption software, hardware and technical information. Companies that operate in a multinational environment can pay a significant price if they are not familiar with these controls.

For instance in the United States encryption controls cover export, but not import or use, of encryption products. A violation of regulations related to the export of encryption may be punishable by fairly serious civil monetary penalties, denial of export privileges or even considerable criminal fines. U.S. law may be violated not only if a product is exported from the United States without authorization, but also if it is "re-exported" from, say, United Kingdom to Afghanistan.

Outside the United States, we have seen numerous governments use informal sanctions to address perceived corporate misuse of encryption technology. In other instances, governments have blocked encrypted communications or confiscated encryption hardware or software. Finally, many of our clients have encountered substantial delays and the inability to deploy or sell encryption products in countries that have established control regimes (such as France and China) – typically because of a lack of familiarity with recent changes in local regulations and procedures.

Because of the vague nature of encryption regulation in many nations (particularly in developing states such as India), some companies doing business in these countries fail to comply fully with the requirements proscribed by the relevant encryption laws. While this may suggest that full compliance is not always necessary, multinational companies that require government licenses and approvals (such as banks and telecommunications companies) simply cannot afford the risks of non- compliance.

An accurate understanding of international encryption regulation can help a company to avoid costs and delays. Understanding the relevant laws and regulations substantially reduces the risk of unintentional violations. In addition an appreciation of the application and approval processes can allow companies to plan ahead and avoid the delays that can result from these processes.

Cambodia

Updated September 12, 2005

Import

Yellow

Use

Green

Export

Yellow

Summary of Encryption Controls in Cambodia

Import Regulations
There are currently no specific regulations on the import of encryption hardware, software and technology to Cambodia. Individuals seeking to import encryption products to Cambodia need only comply with the country's general customs and trade regulations. However, in practice, importers of encryption hardware to Cambodia may be required by the Customs Department to have permission to import such products from the Ministry of Posts and Telecommunications of Cambodia ("MPTC").

Use Regulations
Cambodia does not control the use of encryption technology, whether for confidentiality, authentication or integrity purposes. However, certain Cambodia legislation, while not restricting the use of encryption, may have an effect on how encryption products are used.

Export Regulations
As with imports, there are currently no specific regulations on the export of encryption hardware, software and technology to Cambodia. However, it is the general practice in Cambodia to require exporters to have a permit or license from the MPTC before exporting encryption hardware.

Temporary Imports/Exports
There are no specific regulations on the temporary import or export of encryption products that accompany travelers for their business or personal use (e.g., encryption software on laptop computers) in Cambodia.

Sanctions And Penalties
Cambodian law prescribes penalties for failure to comply with customs laws and trade regulations.

Additional Information
Cambodia is still in the process of recovering after more than 20 years of civil war and communist rule. Although much progress has been made, significant gaps still exist in the nation's legal and institutional framework. The Cambodian government currently imposes few restrictions on imports from abroad and the country enjoys normal trade relations with the United States and many other trading partners.

Details of Encryption Controls in Cambodia

1.1 Introductory Information

Cambodia's constitutional monarchy was re-established in 1993 after more than 20 years of civil war and communist rule. There have been national elections in 1993, 1998 and 2003 and Cambodia is now a developing country with a market economy. Bilateral and multilateral donors support and closely monitor the government's reform program. The International Monetary Fund, World Bank and Asian Development Bank are all active in Cambodia. Although significant gaps exist in the nation's legal and institutional frameworks, Cambodia enjoys normal trade relations with the United States and is a member of the Association of Southeast Asian Nations ("ASEAN"). On October 13, 2004, Cambodia became a member of the World Trade Organization, nearly 10 years after it first applied to join.

1.2 Import

1.2.1 Import Restrictions And Exemptions

There are currently no specific regulations on the import of encryption hardware, software and technology to Cambodia. Individuals seeking to import encryption products to Cambodia need only comply with the country's general customs and trade regulations. However, in practice, importers of encryption "hardware" (but not software or technology) to Cambodia are required by the Customs Department to have permission to import such products from the Ministry of Posts and Telecommunications of Cambodia ("MPTC") prior to clearance at customs.

The Customs Department of Cambodia has a current practice of either prohibiting importation of all kinds of second-hand computer equipment or subjecting such second-hand equipment to twice the import duty of new equipment (30%). The Customs Department would consider second-hand encryption hardware as falling within this general prohibition or increase in duties.

Further, if the importer is a Voice over Internet Protocol ("VoIP") provider, the importation of any technical equipment for provision of VoIP international services must be approved by the MPTC.

1.2.2 Import Approval Process/Licensing

Importers of encryption hardware must submit to the MPTC a written request which provides the technical details on the encryption equipment to be imported. The MPTC will then approve or disapprove (on a case-by-case basis) the specific encryption hardware that has been proposed for importation, inform the importer of the decision, and contact the Customs Department informing them of the approval or disapproval, so as to facilitate the clearance of the imported equipment by the Customs Department once the equipment is sent to Cambodia. This import authorization process normally takes one to two weeks to complete.

1.3 Use

1.3.1 Use Restrictions And Exemptions

There are currently no specific restrictions on the use of encryption hardware and software in Cambodia. The 2002 Draft Sub-Decree on Electronic Transactions seeks to create a legal foundation for commercial electronic transactions and to give legal effect to electronic signatures in Cambodia.

Certain encryption equipment may be considered a technical product related to VoIP. VoIP providers must have a license from the MPTC to provide service in Cambodia (see MPTC Prakas (Decision) 155 on the Organization and Management of Internet and VoIP Services and System, June 19, 2001).

1.3.2 Use Approval Process/Licensing

Not applicable.

1.4 Export

1.4.1 Export Restrictions And Exemptions

As with imports, there are currently no specific regulations on the export of encryption hardware, software and technology to Cambodia. However, it is the general practice in Cambodia to require exporters to have a permit or license from the MPTC before exporting encryption hardware (but not software or technology).

1.4.2 Export Approval Process/Licensing

Exporters of encryption hardware must submit a written request to the MPTC that provides the technical details on the encryption equipment to be exported. The MPTC will then approve or disapprove (on a case-by-case basis) the specific encryption hardware that has been proposed for exportation, inform the exporter of the decision, and contact the Customs Department informing them of the approval or disapproval, so as to facilitate the clearance of the exported equipment by the Customs Department once the equipment is sent from Cambodia. This process normally takes one to two weeks to complete.

1.5 Temporary Import And Export Controls

There are no restrictions on the temporary import or export of encryption software stored on laptop computers carried by business travelers for their business or personal use. However, as mentioned above, the Customs Department has a general practice of prohibiting importation of second-hand computer equipment which is not intended for individual business or personal use.

1.6 Intangible Transfers

There are no controls on the intangible transfer (e.g., Internet download or upload) of encryption software to or from Cambodia.

1.7 Sanctions And Penalties

Cambodian law prescribes penalties for failure to comply with customs laws and trade regulations.

1.8 Additional Information

As noted above, Cambodia is still in the process of recovering from civil war and communist rule. Although there has been much progress, the process is not nearly complete. The 2002 Draft Sub-Decree on Electronic Transactions states that one of the intended purposes of the law is: “To facilitate electronic commerce, eliminate barriers to electronic commerce resulting from uncertainties over writing and signature requirements and to promote the development of the legal and business infrastructure necessary to implement secure electronic commerce.” (Article 2(b) of the Draft Sub-Decree on Electronic Transactions 2002).

Although this draft regulation has not yet come into effect, one may infer from its language that the Cambodian government’s general policy would be to facilitate the importation and use of equipment or technology (such as encryption equipment or technology) that would promote and implement secure electronic commerce.

2.0 Contact Addresses

Further information on Cambodia’s trade and customs regulations and foreign trade policies can be obtained from the following government agencies:

Customs and Excise Department
Norodom Boulevard
Phnom Penh, Cambodia.
Telephone / Facsimile: 855-23-214065
E-mail: customs@camnet.com.kh
Website: **http://www.camnet.com.kh/customs**

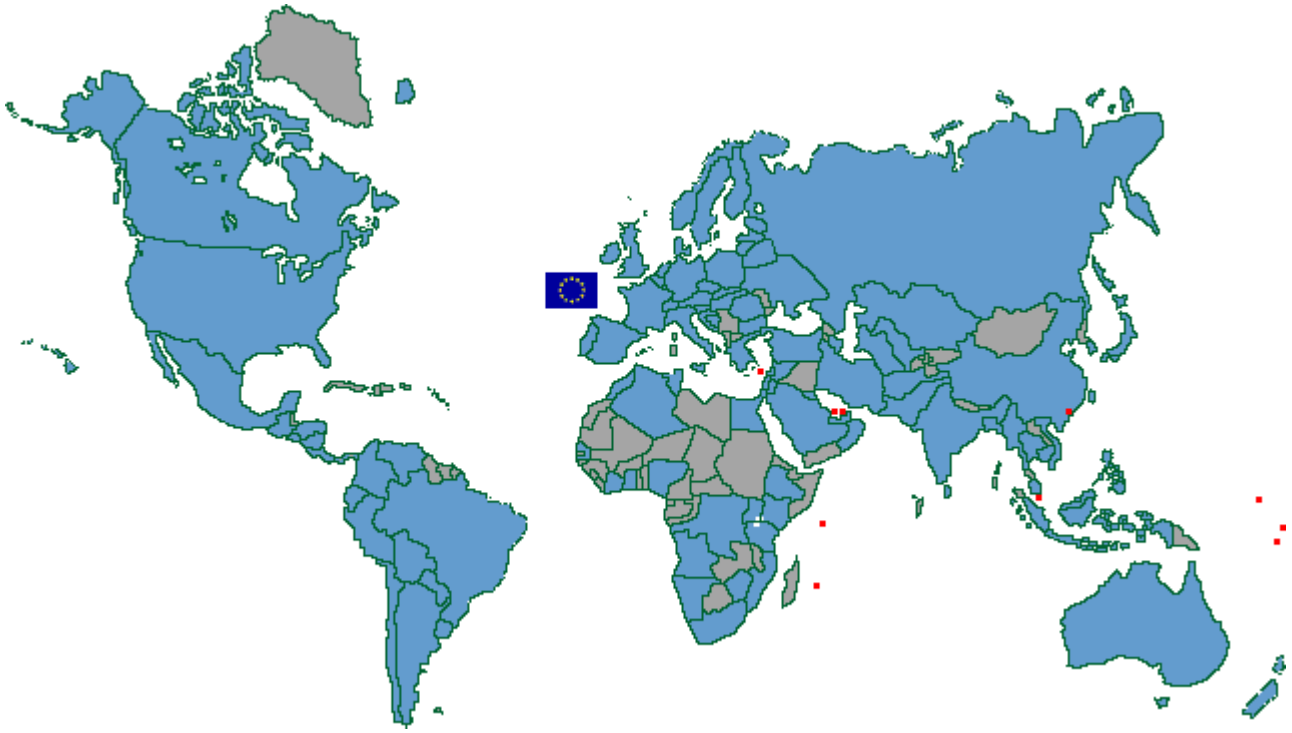
Ministry of Posts and Telecommunications
Corner of Street 13 & 102
Phnom Penh 12202, Cambodia.
Telephone: 855-23-426510 / 855-23-724809
Facsimile: 855-23-426011
Website: **http://www.mptc.gov.kh/**

3.0 References

- Draft Sub-decree on Electronic Transactions, 2002
- Draft Law on Customs, August 15, 2002
- MPTC Prakas 068 BTPrK on the Price and Use of Telecommunications Equipment, March 19, 1998
- MPTC Prakas (Decision) 155 on the Organization and Management of Internet and VoIP Services and System, June 19, 2001

- Royal Kram (Decree) NS-RKM-0702/012 on the Postal Law, July 11, 2002
- Royal Kram NS-RKT-0196/20 on the Creation of the MPTC, January 24, 1996
- Sub Decree No. 38 on Control, Import, Production, Sale, Purchase, Distribution, and Use of all Kinds of
- Weapons and Explosive Substances, April 30, 1999
- Sub Decree No. 66 on the Organization and Function of the MPTC, October 22, 1997
- The Law Regarding Duties on Exported and Imported Goods (Customs and Excise Department), July 20, 1989

Scope of Country Guide to Encryption Regulations



Afghanistan
Algeria
Angola
Argentina
Australia
Austria
Azerbaijan
Bangladesh
Belarus
Belgium
Bolivia
Brazil
Brunei
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cote d'Ivoire
Croatia
Czech Republic
Democratic
Republic of the
Congo (Zaire)
Denmark
Dubai
Ecuador
Egypt
El Salvador
Estonia
Ethiopia
European Union
Finland
France
Germany
Greece
Guatemala
Honduras
Hong Kong
Hungary
Iceland
India
Indonesia
Iran
Ireland
Israel
Italy
Japan
Kazakhstan
Kenya
Kuwait
Latvia
Lithuania
Luxembourg
Malaysia
Mexico
Morocco
Mozambique
Myanmar
(Burma)
Namibia
Netherlands
New Zealand
Nicaragua
Nigeria
Norway
Pakistan
Paraguay
Peru
Philippines
Poland
Portugal
Romania
Russia
Saudi Arabia
Singapore
Slovak Republic
Slovenia
South Africa
South Korea
Spain
Sri Lanka
Sweden
Switzerland
Taiwan
Tanzania
Thailand
Tunisia
Turkey
Turkmenistan
Ukraine
United Kingdom
United States
Uruguay
Uzbekistan
Venezuela
Vietnam
Zimbabwe