

The Value of Understanding International Encryption Regulation

Steptoe & Johnson LLP

1330 Connecticut Avenue, NW
Washington, DC 20036
Tel: 202.429.3000
Fax: 202.429.3902

750 Seventh Avenue
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 20 7367 8000
Fax: +44 20 7367 8001

Encryption technology offers both substantial benefits (by protecting the confidentiality, authenticity, and integrity of business and personal information) and substantial risks (by making it easier for criminals and terrorists to conceal communications regarding illegal behavior). While most countries recognize the benefits of encryption, the associated risks have led many governments to impose controls on the import, use, 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.

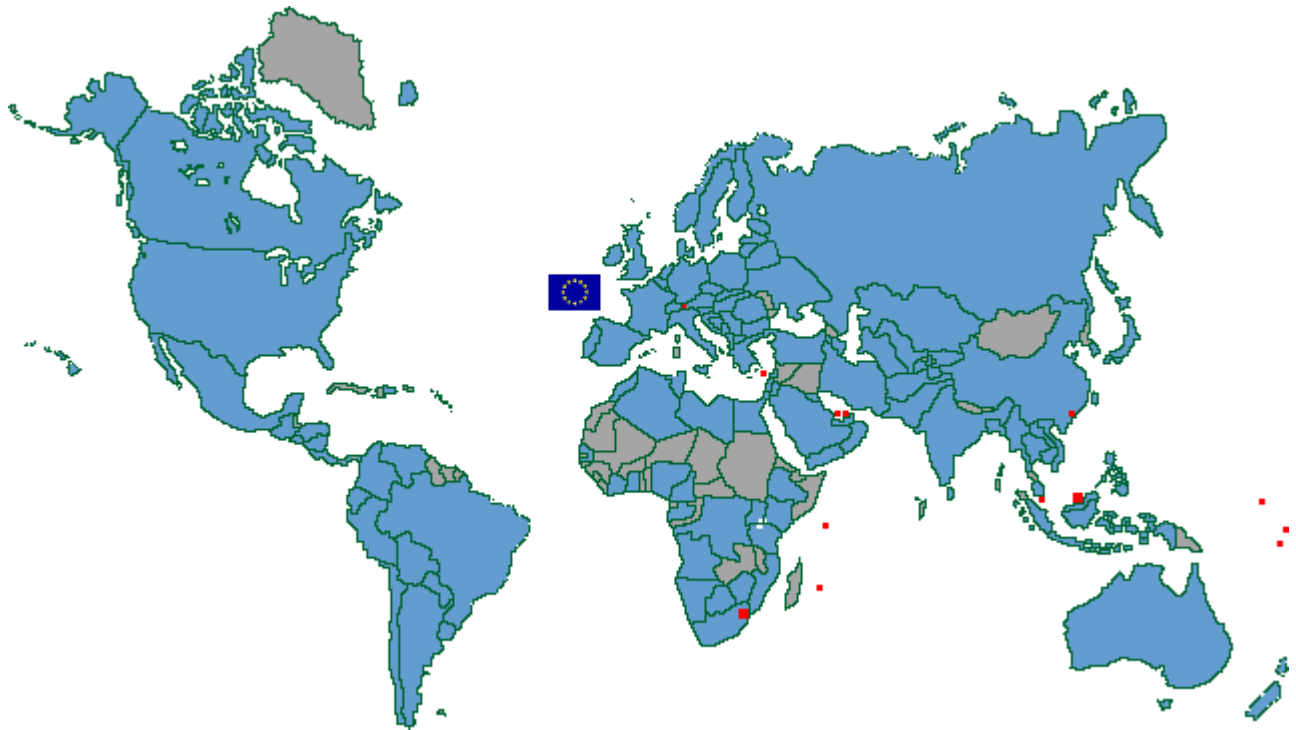
For instance, in the United States encryption controls cover export, but not import or use, of encryption products. A violation of regulations related to the export of encryption may be punishable by civil monetary penalties, denial of export privileges, and criminal fines. US law may be violated not only if a US-origin product is exported from the United States without authorization, but also if it is “re-exported” from another country to a third country.

Outside the United States, numerous governments restrict the import, use, and/or export of encryption. Some countries impose severe sanctions for a violation of their restrictions. Others use informal sanctions to address perceived misuse of encryption technology. In other instances, governments have blocked communications or confiscated encryption hardware or software. Finally, many companies have encountered substantial delays or the inability to deploy or sell encryption products in countries with established control regimes—typically because of a lack of familiarity with recent changes in local regulations and procedures.

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

Steptoe’s subsidiary, InternatLaw L.L.C., offers a comprehensive, online guide to worldwide encryption regulations. The guide contains detailed reports on the encryption regulations of approximately 130 countries. Each report discusses applicable laws and regulations regarding the import, use, and export of encryption, including rules on “internal” corporate use, “intangible” imports and exports (*i.e.*, Internet downloads or uploads), and temporary imports of encryption on laptops or other mobile devices. Each report also covers applicable penalties and provides local points of contact for additional information. A list of countries currently covered by the guide follows.

Scope of Country-by-Country Guide to Encryption Regulation



Afghanistan	Croatia	Italy	Norway	Tajikistan
Albania	Cyprus	Japan	Oman	Tanzania
Algeria	Czech Republic	Jordan	Pakistan	Thailand
Angola	Denmark	Kazakhstan	Panama	Tunisia
Argentina	Dominican Republic	Kenya	Paraguay	Turkey
Armenia	Ecuador	Kuwait	Peru	Turkmenistan
Australia	Egypt	Kyrgyzstan	Philippines	Uganda
Austria	El Salvador	Laos	Poland	Ukraine
Azerbaijan	Estonia	Latvia	Portugal	United Arab Emirates
Bahrain	Ethiopia	Lebanon	Qatar	United Kingdom
Bangladesh	European Union	Libya	Romania	United States of America
Belarus	Fiji	Liechtenstein	Russia	Uruguay
Belgium	Finland	Lithuania	Samoa	Uzbekistan
Bolivia	France	Luxembourg	Saudi Arabia	Venezuela
Bosnia and Herzegovina	Gabon	Macedonia	Senegal	Vietnam
Botswana	Germany	Malaysia	Serbia	Yemen
Brazil	Ghana	Marshall Islands	Seychelles	Zimbabwe
Brunei	Greece	Mauritius	Singapore	
Bulgaria	Guatemala	Mexico	Slovakia	
Cambodia	Honduras	Montenegro	Slovenia	
Cameroon	Hong Kong, S.A.R.	Morocco	South Africa	
Canada	Hungary	Mozambique	South Korea	
Chile	Iceland	Myanmar (Burma)	Spain	
China	India	Namibia	Sri Lanka	
Colombia	Indonesia	Netherlands	Swaziland	
Congo (Dem. Rep.)	Iran	New Zealand	Sweden	
Costa Rica	Ireland	Nicaragua	Switzerland	
Côte d'Ivoire	Israel	Nigeria	Taiwan	

For more information on the guide, or to set up a demonstration, contact [Michael Vatis](#), telephone 212.506.3927, or [Sally Albertazzie](#), telephone 202.429.3062.

Steptoe & Johnson's E-Commerce Practice Group

Steptoe & Johnson LLP

1330 Connecticut Avenue, NW
Washington, DC 20036
Tel: 202.429.3000
Fax: 202.429.3902

750 Seventh Avenue
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 20 7367 8000
Fax: +44 20 7367 8001

Overview

Encryption regulatory issues have been, and will continue to be, a hazardous area for companies attempting to comply with varying regulations around the world. Steptoe & Johnson LLP's E-Commerce Practice Group offers a unique service to clients seeking to navigate worldwide cryptography regulations. We have an international team of lawyers based in both the United States and Europe, whose combined experience spans decades.

As well as being leaders in encryption issues, Steptoe has also developed a broad network of information sources around the world, including government agencies, multilateral organizations such as the OECD, local embassies, commercial networks and organizations, and local counsel. These contacts give us the unique ability to send quick inquiries to numerous countries and to obtain formal or informal guidance about encryption regulations. Our contacts are particularly useful in countries that do not publish the details of their encryption policies. With the help of our extended network, we provide both counseling on country-by-country requirements and assistance in obtaining import, export, or use licenses around the world.

Steptoe & Johnson's E-Commerce Practice Group represents leading financial institutions, information and telecommunications services, hardware and software firms, and other multinational organizations on a wide array of issues concerning privacy, information security, and electronic commerce. This includes litigation, dealings with law enforcement or security agencies, regulatory compliance, internal investigations, and strategic planning.

Michael Vatis is a partner in Steptoe's New York office. His practice focuses on Internet, privacy, security, e-commerce, and technology matters, including issues involving security, intelligence, and law enforcement. He has extensive experience advising clients on US export controls on encryption as well as on foreign jurisdictions' laws governing the importation, use, and export of encryption. 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. He was also Associate Deputy Attorney General at the Department of Justice, where he helped oversee the Department's activities and policies in the areas of national security, counterterrorism, intelligence and counterintelligence, cybercrime, and encryption. 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

Stewart Baker recently rejoined the firm as a partner in Steptoe's Washington, DC office following 3-1/2 years at the Department of Homeland Security as its first Assistant Secretary for Policy. Described by The Washington Post as "one of the most techno-literate lawyers around," Mr. Baker's practice covers national security, electronic surveillance, law enforcement, export control encryption, and related technology issues. He has been a key advisor on US export controls and on foreign import controls on technology. He has also advised companies on the requirements imposed by the Committee on Foreign Investment in the United States. In addition, he was responsible for spearheading the government-private sector coalition that permitted major telecommunications equipment manufacturers and carriers to break the decade-long deadlock with law enforcement on wiretapping of modern technology, permitting successful implementation of the Communications Assistance for Law Enforcement Act ("CALEA").

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.

Julia Court Ryan is Of Counsel in Steptoe's Washington, DC office. For over a decade, Ms. Ryan has advised clients on export control and economic sanctions laws and regulations. She is a key lawyer in Steptoe's encryption practice, advising companies on encryption import, export, and use laws and regulations under US rules and in jurisdictions around the world. Her encryption practice also includes transactional advice, encryption and product classifications.

Maury Shenk is a Technology, Media & Telecommunications consultant and adviser to the London office of Steptoe & Johnson and is a dual-qualified US/UK lawyer. He has extensive experience on regulatory, commercial, transactional and policy matters involving electronic commerce, representing many leading technology companies from the United States and Europe. He

Steptoe & Johnson's E-Commerce Practice Group

advises clients on the legal aspects of business on the Internet, including online agreements, data protection, information security, intellectual property and competition. Maury frequently handles technology transactions, including M&A and outsourcing agreements. He works with Steptoe & Johnson's leading encryption export/import team, and is experienced in encryption licensing proceedings in the US, UK, France, Russia, China and other jurisdictions.

Sally Albertazzie is a specialist in Steptoe's E-Commerce practice group. She has over 15 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. She is a graduate of Georgetown University's Paralegal Institute.

The team has represented numerous companies providing encryption, telecommunications, information services, and electronic payment services on litigation, regulatory, legislative and corporate contractual matters. The team has also advised numerous firms on e-commerce, privacy, data protection, data retention, and consumer protection in the United States, European Union and other jurisdictions.

Our clients include some of the world's most prominent companies in a variety of business endeavors:

- Internet service providers
- Communications providers
- Voice over Internet Protocol providers
- Numerous software and hardware companies
- Global investment and commercial banks
- Energy companies
- Other technology companies